

Anna Otto:

Entwicklung von Datenschutzrollen
für das
Audit Information System
im SAP ERP

Im Folgenden wird ein Auszug aus der gleichnamigen Diplomarbeit dokumentiert, die im Fachbereich Informatik der Universität Hamburg im Februar 2007 eingereicht wurde.

Die Erstellung der Diplomarbeit wurde durch einzelne FORBIT-Mitarbeiter unterstützt.

Diese Kurzfassung beinhaltet die Darstellung der neu entwickelten Rollen und Hinweise zur Implementierung im Unternehmen.

Der folgende Text kann im Betrieb bei der Erstellung von AIS-Prüfrollen für Datenschutzbeauftragte und Betriebs-/Personalräte als Hilfestellung dienen!

Aufgabenstellung

Das Ziel dieser Diplomarbeit besteht in der Entwicklung von Datenschutzrollen für das Audit Information System im SAP ERP. Diese Rollen sollen dem Datenschutzbeauftragten (DSB) hauptsächlich die Überwachung ordnungsgemäßer Programmanwendung in einem SAP ERP-System ermöglichen.

Die Idee zu diesem Diplomarbeitsthema entstand in Gesprächen mit Mitgliedern der Arbeitsgruppe Datenschutz (DSAG¹ Arbeitskreis Revision), die derzeit eine Neufassung des "Leitfaden Datenschutz für SAP R/3, Release 4.6" für SAP ERP erarbeitet. Eine Neukonzeption von Datenschutzrollen wurde im Rahmen der Neufassung des Datenschutzleitfadens vom Redaktionsteam, dem auch der Datenschutzbeauftragte der SAP AG angehört, angeregt.

Keine der Standardrollen des Audit Information System bietet alle Funktionalitäten, die der Datenschutzbeauftragte für die Überwachung der ordnungsgemäßen Programmanwendung benötigt. Der DSB sollte z.B. nur dann Zugang zu personenbezogenen Daten erhalten, wenn dies zur Erfüllung seiner Aufgaben notwendig ist. Eine derartige Differenzierung ist mit den SAP-Standardrollen nicht möglich. Ebenfalls problematisch sind die teilweise in den Rollen enthaltenen Änderungsberechtigungen.

Die technische Ausarbeitung der Diplomarbeit erfolgte mit einem IDES-Testsystem (IDES mySAP ERP 2004 (ECC 5.0)), in dem die AIS-Standardrollen analysiert und neue Datenschutzrollen entwickelt wurden. Auf einzelne Besonderheiten bei der Rollenentwicklung, die mit der Verwendung des IDES-Testsystem verbunden sind, wird in in dem Abschnitt zur Vergabe und Ausprägung der Rollen hingewiesen.

Für meine Diplomarbeit habe ich insgesamt sieben Datenschutzrollen entwickelt, deren Funktionalitäten ich im folgenden Text kurz beschreibe. Die Datenschutzrollen wurden in Transaktionsrollen und Berechtigungsrollen getrennt, da dieses Vorgehen bei den Standardrollen des AIS ebenfalls gewählt wurde. Ausserdem gehe ich darauf ein wie die Rollen vergeben werden sollten und inwiefern sie noch ausgeprägt werden müssen.

¹DSAG, Deutschsprachige SAP®Anwendergruppe e.V., <http://www.dsag.de/>

Entwicklung von Rollen für den Datenschutzbeauftragten

Konzeption der Rollen

Die Konzeption der neuen Rollen für den Datenschutzbeauftragten ist in vier Schritten erfolgt.

1. Die Analyse der von SAP mit dem Audit Information System ausgelieferten Standardrollen lieferte einen Überblick über die vorhandenen Funktionen des Audits.
2. Anhand der in Kapitel 4 erarbeiteten Informationen wurden die für den DSB relevanten SAP-Funktionalitäten zusammengetragen und mit unterschiedlichen Berechtigungen getestet. Insbesondere die Transaktionen, die einen erheblichen Teil der Berechtigungsrollen ausmachen, mussten auf mögliche Änderungsrechte überprüft werden.
3. In diesem Schritt wurden die ausgewählten Funktionalitäten den drei Transaktionsrollen zugeordnet, die im folgenden beschrieben werden:
 - Z_AUDITOR_DSB_DIS für die Funktionen, die mit reinen Anzeigeberechtigungen ausführbar sind
 - Z_AUDITOR_DSB_HR_DIS für die Funktionen, die mit reinen Anzeigeberechtigungen ausführbar sind, aber auch Zugriff auf personenbezogene Daten insbesondere im SAP HR ermöglichen
 - Z_AUDITOR_DSB_ALL für alle Funktionen der vorherigen Rollen, erweitert um die Funktionen, die nur mit Änderungsberechtigungen ausführbar sind.

Die Transaktionsrollen sind so gestaltet, dass die Funktionalitäten der Rolle Z_AUDITOR_DSB_DIS vollständig in den Menüs der anderen beiden Rollen enthalten sind. Diese Beziehung besteht ebenso zwischen den Menüs der Rollen Z_AUDITOR_DSB_HR_DIS und Z_AUDITOR_DSB_ALL. Um die inhaltliche Zuordnung in der Menüstruktur nicht zu unterbrechen, musste eine derartige Vorgehensweise gewählt werden.

4. Im letzten Schritt wurden die neuen Berechtigungsrollen entworfen:

- Z_AUDITOR_DSB_DIS_A beinhaltet die reinen Leseberechtigungen zu den Funktionen der Transaktionsrolle
- Z_AUDITOR_DSB_HR_DIS_A beinhaltet die reinen Leseberechtigungen zu den Funktionen der Transaktionsrolle, inklusive der personenbezogenen Daten
- Z_AUDITOR_DSB_ALL_A beinhaltet die Berechtigungen zu den Funktionen der Transaktionsrolle, auch solche, die kritische Änderungen zulassen.

Im Gegensatz zu den Transaktionsrollen wurden die Berechtigungsrollen so konzipiert, dass die jeweiligen Berechtigungen sich nicht überschneiden. Dies erleichtert die Anpassung im Betrieb.

Die oben dargestellte Unterteilung der SAP-Funktionalitäten wurde gewählt, um eine differenzierte Zuteilung dieser Rollen zu ermöglichen.

Durch die Vergabe der Z_AUDITOR_DSB_DIS-Rolle in Kombination mit der Rolle Z_AUDITOR_DSB_DIS_A erhält der betriebliche Datenschutzbeauftragte reine Anzeigefunktionen zur Auditierung eines SAP-Systems.

Da der Datenschutzbeauftragte nur in bestimmten Prüfungssituationen auf personenbezogene Daten zugreifen muss, ist es sinnvoll, die hierfür erforderlichen Funktionalitäten in eine zweite Rollenkategorie auszulagern. Diese beinhaltet die Rollen Z_AUDITOR_DSB_HR_DIS und Z_AUDITOR_DSB_HR_DIS_A, womit neben reinen Anzeigeberechtigungen auch Zugriffe auf personenbezogene Daten insbesondere im SAP HR verbunden sind. Dieses Vorgehen wurde auch im Leitfaden Datenschutz empfohlen. Dort heißt es: „Der Datenschutzbeauftragte sollte grundsätzlich über eine "Grundrolle für Datenschutzbeauftragte" verfügen. Diese umfasst die für eine Datenschutzsystemprüfung erforderlichen umfassenden Leserechte im Audit-Informationssystem [...] sowie den direkten Aufruf der entsprechenden Transaktionen und Reports, allerdings keinen Zugriff auf Mitarbeiterdaten. Darüber hinaus kann dem Datenschutzbeauftragten für Echtdatenprüfungen eine zweite auf die individuellen Zuständigkeiten geschaffene Rolle zugeteilt werden.“

In der dritten Rollenkategorie wurden die für den DSB sinnvollen Funktionalitäten zusammengetragen, unabhängig davon, ob damit auch Änderungsberechtigungen oder kritische Aktivitäten verbunden sind. Die entsprechenden Rollen Z_AUDITOR_DSB_ALL und Z_AUDITOR_DSB_ALL_A wurden aufgrund der Unzulänglichkeiten des SAP-Systems erstellt, auf die in vorherigen Kapiteln ausführlich hingewiesen wurde.

Die Menüpunkte der Transaktionsrollen sind aus den in Kapitel 4.2 beschriebenen Standardrollen abgeleitet. Die dort enthaltenen Mappen und Transaktionen wurden zusammengefasst und neu strukturiert. Um das Menü für den Datenschutzbeauftragten übersichtlicher zu gestalten, sind die Mappen nach Themen gegliedert und die Transaktionen wurden entsprechend zugeordnet.

In einigen Menüs der Transaktionsrollen wurden zusätzliche Funktionalitäten hinzugefügt, die in den oben beschriebenen Standardrollen von SAP nicht enthalten sind. Diese sind:

- Der Mappe "HR: Protokollierung"² wurde eine Untermappe hinzugefügt, welche die Transaktion "SE17" enthält. In der Beschreibung dieser Transaktion wird auf die Tabelle "AQPROT" verwiesen, welche die Protokolldatensätze zu den Queries anzeigt. Dies ist nur sinnvoll, wenn die Protokollierung von Queries aktiviert ist, was für einzelne Datenfelder aus der HR Datenbank der Fall sein sollte. Eine Transaktion oder einen Report gibt es für diese Information nicht, deswegen muss der Umweg über den "Data Browser" ("SE17") genommen werden.
- Der Mappe "Benutzer und Berechtigungen" wurde die erzeugte Transaktion "RSHUSERRELATIONS" hinzugefügt. Wie bereits in Kapitel 3.3 ausgeführt, bietet der Report "RSHUSERRELATIONS" einen Überblick über alle vorhandenen HR-Berechtigungsprofile, d.h. inklusive der strukturellen Berechtigungen. Da es nicht möglich ist, Reports in Transaktions- oder Berechtigungsrollen einzubinden, muss aus dem Report eine Transaktion erzeugt werden. Diese Transaktion gilt aber nur für den entsprechenden Mandanten, in diesem Fall unter der Bezeichnung "Y_I10_68000200".
- In der Mappe "Einführung in das AIS" sind Links mit Informationen zu den Fragestellungen des Audits enthalten. Zu den bereits vorhandenen wurden unter anderem die Adresse des Datenschutzbeauftragten des Bundes und die der Europäischen Kommission zum Bereich Datenschutz eingefügt.³

Auf den folgenden Seiten sind die entwickelten Rollen tabellarisch dargestellt. In den Tabellen 0.1 und 0.2 ist die Strukturierung der Benutzermenüs durch die Transaktionsrollen beschrieben und die Tabellen 0.3 und 0.4 geben einen Einblick in die Berechtigungen der Berechtigungsrollen.

In der Abbildung 0.1 wird ein Überblick über die Menüstruktur der Rolle Z_AUDITOR_DSB_DIS gegeben. Die Berechtigungen der Z_AUDITOR_DSB_DIS_A-Rolle sind in Abbildung 0.2 zu sehen. Eine komplette Dokumentation aller neu konzipierten Rollen ist aus Gründen der Übersichtlichkeit in den Anhängen E und F der vollständigen Fassung der Diplomarbeit zu finden. In diesem Text sind die Rollen mit Lesezugang Z_AUDITOR_DSB_DIS und Z_AUDITOR_DSB_DIS_A dokumentiert. Ausserdem werden noch die Berechtigungen der Rollen Z_AUDITOR_DSB_HR_DIS_A und Z_AUDITOR_DSB_ALL_A dargestellt.

²in der Rolle Z_AUDITOR_DSB_HR_DIS enthalten

³Die Links waren am 15.12.2006 gültig.

Transaktionsrolle	Funktionsumfang
Z_AUDITOR_DSB_DIS	<p>Diese Rolle definiert ein Benutzermenü, das nur Zugang zu SAP-Funktionen bietet, die mit reinen Anzeigeberechtigungen ausführbar sind.</p> <p>Das Benutzermenü enthält:</p> <ul style="list-style-type: none"> - die Mappe Einführung in das AIS, mit den Untermappen: Allgemeine Informationen, AIS Bedienungshinweise, AIS Administration und Internet-Links; - die Mappe Allgemeine Systemprüfungen, mit den Untermappen: Systemübersicht/Systemlandschaft (enthält die Mappen der System Konfiguration), Systemverbund und Transporte (insbesondere das Transport Management System) und Sicherheitseinstellungen und -tools (insbesondere die Top Security Reports); - die Mappe Entwicklung/Customizing, mit den Untermappen: ABAP Programme, Transaktionen (enthält die Transaktion "RSAUDITC_BCE - Gesperrte Transaktionen") und Erweiterungskonzept; - die Mappe Repository/Tabellen, mit den Untermappen Informationen/Überblick (insbesondere mit der Transaktion "SE84 - Repository Infosystem"), Tabellenberechtigung, Tabellenaufzeichnungen und Zugriffstatistik; - die Mappe Protokollierung, mit den Untermappen Systemprotokolle und Statusanzeigen (insbesondere mit der Transaktion "SM21 - Systemprotokolldatei") und Hintergrundverarbeitung; - die Mappe Benutzer und Berechtigungen, insbesondere mit der Untermappe Infosystem Benutzer & Berechtigungen und der Transaktion "Y_RHUSERRELATIONS"; - die Mappe HR-Personalwirtschaft, mit den Untermappen Personaladministration (mit Transaktionen zu den Infotypen) und Personalplanung; - und die Mappe Übersichten gemäß BDSG, mit den Dateiregistern zu personenbezogenen Daten.

Tabelle 0.1: Überblick über die Funktionen der entwickelten Transaktionsrollen

Transaktionsrolle	Funktionsumfang
Z_AUDITOR_DSB_HR_DIS	<p>Diese Rolle definiert ein Benutzermenü, das nur Zugang zu Funktionen bietet, die mit reinen Anzeigeberechtigungen ausführbar sind. Ausserdem wird der Zugang zu personenbezogenen Daten ermöglicht.</p> <p>Die Mappenstruktur ist die gleiche wie in der Rolle Z_AUDITOR_DSB_DIS, d.h. deren Mappen und Transaktionen sind auch in dieser Rolle enthalten.</p> <p>Als Erweiterung bietet diese Rolle hauptsächlich die Mappe HR-Protokollierung und die Untermappe Personaldaten zur Mappe Personaladministration, hier kann z.B das Personalstammblatt eines Mitarbeiters eingesehen werden.</p> <p>An einigen Stellen sind in dieser Rolle Transaktionen enthalten, die eine Leistungsanalyse erlauben. Diese Transaktionen verteilen sich über das gesamte Menü und sind nicht in der Rolle Z_AUDITOR_DSB_DIS enthalten.</p>
Z_AUDITOR_DSB_ALL	<p>Diese Rolle definiert ein Benutzermenü, das Zugang zu relevanten Funktionen bietet, die nur mit Änderungs-berechtigungen ausführbar sind. Ausserdem wird der Zugang zu personenbezogenen Daten ermöglicht.</p> <p>Die Mappenstruktur ist die gleiche wie in den beiden anderen Transaktionsrollen, d.h. deren Mappen und Transaktionen sind auch in dieser Rolle enthalten.</p> <p>Als Erweiterung bietet diese Rolle hauptsächlich Transaktionen, die nur mit Änderungsrechten ausführbar sind, oder Änderungen ermöglichen. Diese Transaktionen verteilen sich über das gesamte Menü und sind nicht in den anderen beiden Rollen enthalten. Beispiele für solche Transaktionen sind:</p> <ul style="list-style-type: none"> - in der Mappe Sicherheitseinstellungen und -tools die Top Security Reports: "RSRFCCHK - RFC Destinations mit Anmeldedaten", "SE03 - Transport Organizer Tools"; - in der Mappe Systemübersicht/Systemlandschaft die Transaktion zu den Mandantenkopie Protokollen: "SCC3 - Mandantenkopie Protokoll", die das Löschen der Protokolle ermöglicht. <p>An einigen Stellen sind aber auch neue Untermappen eingefügt, wie die Untermappe zu den Internet Benutzern in der Mappe Benutzer und Berechtigungen.</p>

Tabelle 0.2: Überblick über die Funktionen der entwickelten Transaktionsrollen

Berechtigungsrolle	Funktionsumfang
Z_AUDITOR_DSB_DIS_A	<p>Diese Rolle definiert Leseberechtigungen zu den Funktionen, die im Benutzermenü der Transaktionsrolle Z_AUDITOR_DSB_DIS enthalten sind.</p> <p>Es gibt Berechtigungen:</p> <ul style="list-style-type: none"> - zu anwendungsübergreifenden Berechtigungsobjekten, dies beinhaltet insbesondere die Anzeige der Funktionen des Verteilungsmodells (ALE), die inaktive Berechtigung zum RFC-Zugriff (diese Berechtigung muss noch vom Unternehmen gepflegt werden) und die fünf verschiedenen Berechtigungen zur Transaktionscode-Prüfung beim Transaktionsstart; - zur Basis - Administration, dies beinhaltet insbesondere einige Systemberechtigungen, die Anzeige der Archivierung der Basiskomponente, die Berechtigung zum Export aus dem SAP GUI, die Berechtigungen zur Spoolerverwendung (z.T ungepflegt, die Geräteberechtigung muss z.B. noch angepasst werden), die Tabellenpflege (mit zwei verschiedenen Berechtigungen als Vorschlag, die beide nur eine Anzeige ermöglichen), die Berechtigung zum Anzeigen der Sonderbenutzer in der Benutzer- und Berechtigungsverwaltung und Anzeigen der Benutzerstammpflege; - zur Basis - Entwicklungsumgebung, dies beinhaltet die Anzeige des ABAP Workbench ("S_DEVELOP"), die ABAP Programmablaufprüfung (die Berechtigung hat nur den Wert "SUBMIT") und die Anzeige des "Transport Organizer"); - zu Basis - Zentrale Funktionen, dies beinhaltet insbesondere die Anzeige der Nummernkreise, die Anzeige der Änderungsbelege zum Datenexport mit RFC im Mandantenvergleich (und -kopien) und die inaktive Berechtigung zur Anzeige von Dokumenten (diese Berechtigung muss noch vom Unternehmen gepflegt werden).

Tabelle 0.3: Überblick über die Funktionen der entwickelten Berechtigungsrollen

Berechtigungsrolle	Funktionsumfang
Z_AUDITOR_DSB_HR_DIS_A	<p>Diese Rolle definiert Leseberechtigungen zu den Funktionen, die im Benutzermenü der Transaktionsrolle Z_AUDITOR_DSB_HR_DIS bereitgestellt werden. Sie enthält nur Berechtigungen die in der Z_AUDITOR_DSB_DIS_A-Rolle nicht vorhanden sind und stellt so eine Erweiterung dar.</p> <p>Es gibt Berechtigungen:</p> <ul style="list-style-type: none"> - zu anwendungsübergreifenden Berechtigungsobjekten, dies beinhaltet die zwei verschiedenen Berechtigungen zur Transaktionscode-Prüfung beim Transaktionsstart; - zur Basis - Administration, dies beinhaltet die Anzeige der Archive, die Tabellenpflege (nur eine Anzeige wird ermöglicht) und die Anzeige des "Tools Performance Monitor"; - zu Basis - Zentrale Funktionen, dies beinhaltet insbesondere die Anzeige des Anwendungs-Log, die Anzeige der Änderungsbelege und die inaktive Berechtigung zur Anzeige von Dokumenten (diese Berechtigung muss vom Unternehmen gepflegt werden); - zum Personalwesen (dies beinhaltet die Personalplanung für alle Infotypen, Leseberechtigung für alle HR-Stammdaten, Leseberechtigung für Bereiche des HR-Clusters und Ausführen bestimmter HR-Transaktionscodes).
Z_AUDITOR_DSB_ALL_A	<p>Diese Rolle beinhaltet die Berechtigungen zu den Funktionen, die im Benutzermenü der Transaktionsrolle Z_AUDITOR_DSB_ALL bereitgestellt werden. Auch zu solchen, die kritische Änderungen zulassen. Sie enthält nur Berechtigungen die in den anderen beiden Berechtigungsrollen nicht vorhanden sind.</p> <p>Es gibt Berechtigungen:</p> <ul style="list-style-type: none"> - zu anwendungsübergreifenden Berechtigungsobjekten, dies beinhaltet eine Berechtigung zur Transaktionscode-Prüfung beim Transaktionsstart; - zur Basis - Administration, dies beinhaltet eine Systemberechtigung, einige Administrationsberechtigungen im "Change & Transport System" und das Ausführen logischer Betriebssystemkommandos.

Tabelle 0.4: Überblick über die Funktionen der entwickelten Berechtigungsrollen

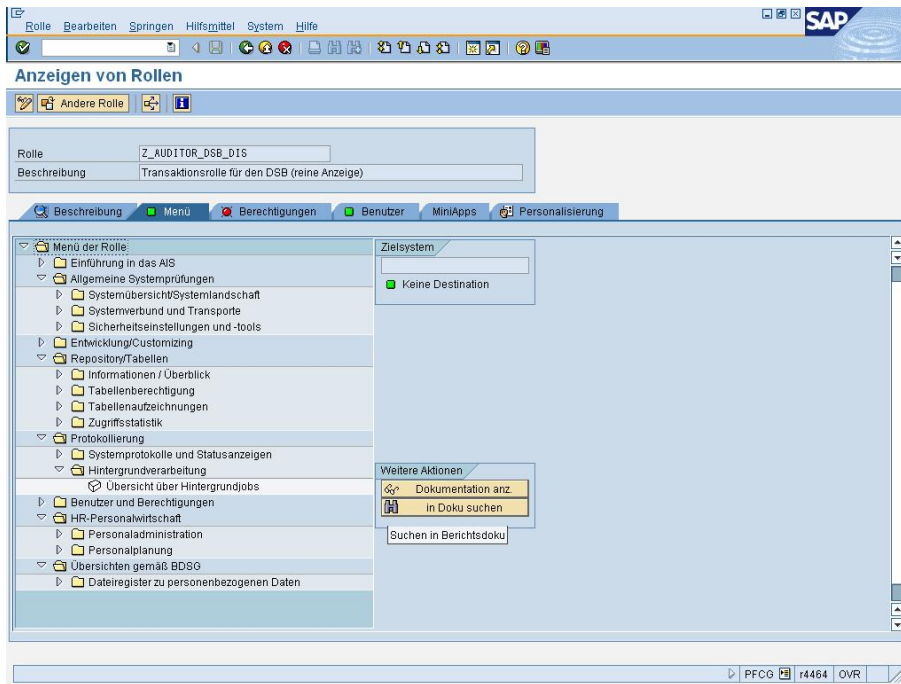


Abbildung 0.1: Menü der Transaktionsrolle Z_AUDITOR_DSB_DIS (Überblick), Screenshot aus SAP ERP vom 07.01.2007.

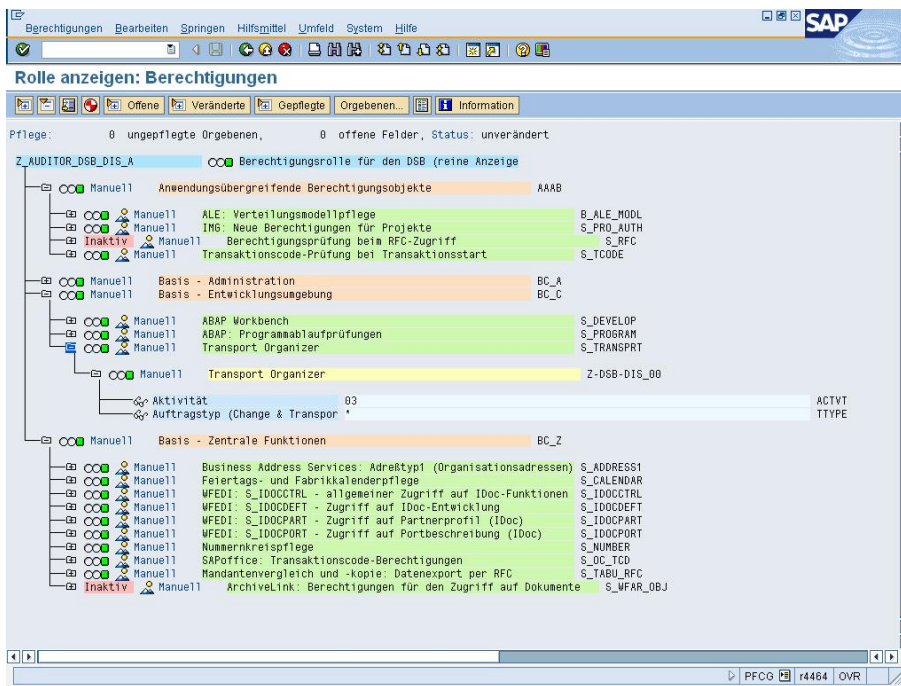


Abbildung 0.2: Berechtigungen der Berechtigungsrolle Z_AUDITOR_DSB_DIS_A (Überblick), Screenshot aus SAP ERP vom 07.01.2007.

Hinweise zur Vergabe und Ausprägung der Rollen

Die Vergabe der Rollen Z_AUDITOR_DSB_HR_DIS und Z_AUDITOR_DSB_HR_DIS_A sollte unter Beachtung der konkreten Aufgabenstellung des DSB und ggf. zeitlich befristet erfolgen. Insbesondere die Rollen Z_AUDITOR_DSB_ALL und Z_AUDITOR_DSB_ALL_A sollten nur unter Einhaltung des 4-Augen-Prinzips und bei entsprechender Protokollierung der Aktivitäten vergeben werden. Als Alternative zur Vergabe dieser Rollen an den DSB bietet sich ein Teil-Audit mit Hilfe eines Administrators an, der über die entsprechenden Berechtigungen verfügt.

Auf die Zuordnung der Transaktions- und Berechtigungsrollen zu einem Benutzer wird im Abschnitt Vergabe der Rollen an Musterbenutzer eingegangen.

In den Berechtigungsrollen müssen einzelne Berechtigungen noch ausgeprägt werden, da sie von den Einstellungen des eingesetzten SAP-Systems bzw. den organisatorischen Gegebenheiten des jeweiligen Unternehmens abhängen.

In der Rolle Z_AUDITOR_DSB_DIS_A ist die Berechtigung zum Berechtigungsobjekt "S_SPO_DEV" ("Spooler: Geräteberechtigungen") nachzubearbeiten. Im Feld "SPO DEVICE" werden die Ausgabegeräte eingetragen, für die der DSB berechtigt sein soll. Momentan ist dieses Feld mit einem "*" für alle Geräte belegt. Diese Berechtigung ist zunächst inaktiv gesetzt worden, weil sie nachgepflegt werden sollte.

Die Berechtigung zum Objekt "S_WFAR_OBJ" (Zugriff auf Dokumente) muss ebenfalls auf die Bedingungen im Unternehmen angepasst werden. Eventuell sollte der DSB nicht auf alle vorhandenen Dokumente zugreifen oder diese bei Personenbezug nur in bestimmten Fällen einsehen können. Daher ist diese Berechtigung zwar in den Rollen Z_AUDITOR_DSB_DIS_A und Z_AUDITOR_DSB_HR_DIS_A enthalten, aber in beiden Fällen inaktiv gesetzt, da sie noch gepflegt werden müssen.

Die in einem SAP ERP-System verwendeten Tabellen werden im Rahmen des Customizing unternehmensspezifisch angepasst. Daher lassen sich auch die Berechtigungen zum Objekt "S_TABU_DIS" standardmäßig nicht vollständig vorgeben. Deshalb wurden in der Rolle Z_AUDITOR_DSB_DIS_A zu dem Tabellen-Berechtigungsobjekt beispielhaft zwei verschiedene Berechtigungen definiert:

1. Für ausgewählte Tabellenberechtigungsgruppen der HR-Personalwirtschaft bzw. des Basissystems ("PC*", "LDAP", "S*") wurde eine Anzeigeberechtigung aktiviert, ohne Zugriff auf personenbezogene Daten.⁴

⁴Die eingetragenen Tabellenberechtigungsgruppen sind nur als Vorschläge zu betrachten. Die Selektion "PC*" beinhaltet viele Tabellen aus den Auswahlbereichen "T5*" und "T70*-T79*", die zur Strukturierung des HR-Moduls verwendet werden, aber keine personenbezogenen Angaben enthalten. Grundlegende Systemtabellen aus dem Auswahlbereich "T0*" sind in "S*" enthalten.

Vorsicht ist bei der Vergabe aller T-Tabellen geboten (z.B. im Rahmen einer betriebsspezifischen Tabellenberechtigungsgruppe), da hierzu auch die Tabellen mit ärztlichen Untersuchungsergebnissen ("T7EHS*") gehören. Ebenfalls höchst kritisch ist die Tabellenberechtigungsgruppe "EHS*" zur Arbeitsmedizin. Im verwendeten SAP ERP-System existieren mehr als 20900 Tabellen (Selektionsparameter: Tabellename von "/*" bis "X*"; Sprachenschlüssel: "DE"), die im Rahmen dieser Diplomarbeit nicht alle gesichtet werden konnten.

2. Exemplarisch sind einzelne Tabellenberechtigungsgruppen für Customizing bzw. SAP-Module (z.B. Finanzwesen, Controlling, Materialwirtschaft) in der zweiten Berechtigung vergeben worden, die inaktiv gesetzt wurde.

In der Rolle Z_AUDITOR_DSB_HR_DIS_A wurde zum Berechtigungsobjekt "S_TABU_DIS" eine Berechtigung aktiviert, welche die Tabellenberechtigungen "AQPR" (Query-Protokollierung), "HRP*" (Infotypen Personalentwicklung), "PA*" (Infotypen Personaladministration) und "PB*" (Infotypen Bewerberverwaltung) umfasst.

In der Berechtigung zum Objekt "S_RFC" (RFC-Zugriff) wird festgelegt, welche RFC-Objekte oder -Typen der Datenschutzbeauftragte ausführen darf. Vorerst wurden keine Werte eingetragen und daher die Berechtigung inaktiv gesetzt. Die für den DSB zulässigen RFC-Objekte müssen in das Feld "RFC_NAME" eingepflegt werden.

In den Kapiteln 3.3 und 4.4 wurde bereits auf die Problematik des Berechtigungsobjekts zum "Change & Transport System" ("S_CTS_ADMI") eingegangen. Auf Grund der mangelnden Differenzierungsmöglichkeit des Berechtigungsobjekts ist eine entsprechende Berechtigung nur in der Rolle Z_AUDITOR_DSB_ALL_A enthalten. Dabei wurden die Änderungsrechte soweit wie möglich eingeschränkt. Die Vergabe einer reinen Anzeigeberechtigung ist nicht möglich.

Die Berechtigungen zu den Objekten "S_TOOLS_EX" ("Tools Performance Monitor"), "S_APPL_LOG" ("Anwendungs-Log") und "S_SCDO" ("Änderungsbelege") ermöglichen, je nach Einstellung der entsprechenden Protokollierung, eine Leistungs- und Verhaltenskontrolle. Aus diesem Grund sind die Berechtigungen in der Rolle Z_AUDITOR_DSB_HR_DIS_A enthalten, aber nicht in der Z_AUDITOR_DSB_DIS_A-Rolle.

Über das Berechtigungsobjekt zur Archivierung ("S_ARCHIVE") kann der Zugang zu personenbezogenen Daten ermöglicht werden. Daher bietet die Rolle Z_AUDITOR_DSB_DIS_A nur Zugriff auf die Archivierung von Objekten des Basissystems, während in der Z_AUDITOR_DSB_HR_DIS_A-Rolle auch weitere relevante Arbeitsgebiete eingesehen werden können.

Die Berechtigungen zu den Objekten "P_ORGIN" (HR-Stammdaten) und "P_PCLX" (HR-Cluster) bieten Anzeigeberechtigungen zu den personenbezogenen Daten der Mitarbeiter und sind daher in der Rolle Z_AUDITOR_DSB_HR_DIS_A enthalten. Diese Berechtigungen müssen an die Gegebenheiten im Unternehmen angepasst werden, z.B. durch Pflege der Mitarbeitergruppen oder Bereichskennungen, auf welche der DSB Zugriff haben soll. In der Berechtigung zum Objekt "PLOG" (Personalplanung) wurde die Planvariante auf den Wert "01 - aktueller Plan" eingestellt. Wenn im Unternehmen von

dieser Einstellung abgewichen werden soll, muss dies entsprechend geändert werden. Je nach Einstellung des SAP HR-Systems sind ggf. Berechtigungen zu weiteren Berechtigungsobjekten zu erteilen, wie z.B. "P_ORG XX", "P_PERNR", "P_ORGINCON", "PLOG_CON" oder "P_ORGXXCON".

Grundsätzlich sind alle Transaktionen, die einen Zugriff auf Änderungsbelege oder Protokolle erlauben, nur in der Rolle Z_AUDITOR_DSB_HR_DIS_A enthalten, da sie eine Leistungs- und Verhaltenskontrolle ermöglichen könnten.

Allerdings wird in der Berechtigungsrolle Z_AUDITOR_DSB_DIS_A der Zugriff auf Änderungsbelege im Rahmen der Benutzerverwaltung erlaubt, weil diese Anzeige für ein Datenschutzaudit elementar ist und hierdurch vermieden werden kann, dass die ergänzende Rolle Z_AUDITOR_DSB_HR_DIS_A bei jeder Prüfung verwendet werden muss.

Um dem Anwenderbetrieb bei der Rollenausprägung den Überblick und die eventuelle Trennung der Z_AUDITOR_DSB_HR_DIS_A-Rolle zu erleichtern, wurden zwei Transaktionsberechtigungen geschaffen, die zwischen Transaktionszugriff auf Benutzerdaten⁵ und HR-Daten unterscheiden.

Ein entsprechendes Differenzierungsverfahren findet auch in der Rolle Z_AUDITOR_DSB_DIS_A Anwendung, wobei fünf verschiedene Berechtigungen zum Objekt "S_TCODE" definiert wurden. Sie erlauben den Zugriff auf die Transaktionen der Bereiche: Basis, Display, Infosystem Benutzer & Berechtigungen und Datenschutz (Dateiregister/Übersichten). Die fünfte Berechtigung zur zentralen Benutzerverwaltung ist inaktiv gesetzt. Sie enthält die Transaktionen ("S_BIE_59000197, S_BIE_59000198, S_BIE_59000199"). Diese sind für die Überprüfung sinnvoll, aber auf Grund der Einstellungen des verwendeten SAP-Testsystems war es nicht möglich, diese Funktionalitäten zu testen. Anwender müssen diese Transaktionen ggf. selbst testen und dann aktivieren. Zu den Transaktionen gibt es ein korrespondierendes Berechtigungsobjekt "S_USER_SYS" (zentrale Benutzerpflege). Die entsprechende Berechtigung ist ebenfalls inaktiv. Wird im Unternehmen eine zentrale Benutzerpflege eingesetzt, sollte dieses Berechtigungsobjekt aktiviert werden.

Um dem Datenschutzbeauftragten die Anwendung der Auditfunktionen zu erleichtern, wurden die einzelnen Transaktionen des "Infosystem Benutzer & Berechtigungen" in die Z_AUDITOR_DSB_DIS-Rolle integriert. Bei Verwendung der Transaktion "SUIM - Benutzerinformationssystem" müsste sich der DSB auf eine andere Bedienungsfläche einstellen.

⁵Hierzu zählt die Transaktion "SM20 - Auswertung Security Audit Log", womit vor allem die Aktivitäten von Notfallbenutzern und Administratoren protokolliert werden sollten. Diese Protokollierung ist insbesondere auch unter Solvency II Gesichtspunkten wichtig (Stichwort: Nachvollziehbarkeit).

Mit der Transaktion "RSUSR003" lässt sich überprüfen, ob die Kennwörter der Standardbenutzer der einzelnen SAP-Mandanten geändert wurden.⁶ Diese Transaktion ist deshalb sicherheitskritisch und sollte nur an spezielle Benutzer vergeben werden. Der Datenschutzbeauftragte sollte aber zu diesen Benutzern gehören, da mangelnde Pflege der Standardbenutzer auch ein erhebliches Risiko unter Datenschutzgesichtspunkten bedeutet. Diese Transaktion ist auch für Prüfungen im Zusammenhang mit Solvency II, Basel II, KonTraG und SOX sinnvoll.

Eine weitere für den DSB interessante Anzeige bietet die Transaktion "RSWBO004 - Systemänderbarkeit setzen". Sie ermöglicht es, entgegen ihrer Beschreibung, nicht die Einstellungen zur Systemänderbarkeit zu verändern,⁷ sondern nur diese zu überprüfen. Die Systemänderbarkeit sollte vom DSB überwacht werden.

Die Transaktion "RSWBOSSR - Aufträge/Aufgaben suchen" konnte nicht getestet werden, da auch bei umfangreichen Berechtigungen das Programm wieder in das Benutzermenü zurückspringt, ohne Informationen anzuzeigen. Für dieses Verhalten konnte keine Erklärung gefunden werden.

Vergabe der Rollen an Musterbenutzer

Die Transaktionsrollen wurden so entworfen, dass sie jeweils ein zusammenhängendes Benutzermenü definieren. Es sollte immer nur eine Transaktionsrolle vergeben werden, da jede Rolle alle notwendigen Funktionen bereitstellt. Ansonsten reihen sich die einzelnen Menüs der Transaktionsrollen aneinander und es entsteht ein unübersichtliches Benutzermenü.

Die Berechtigungsrollen sind aus Gründen der Übersichtlichkeit nicht redundant zueinander. Um z.B. die vollständigen Berechtigungen für die Transaktionsrolle Z_AUDITOR_DSB_ALL zu erhalten, müssen alle drei Berechtigungsrollen vergeben werden. Dieser Aufbau der Berechtigungsrollen erleichtert die Ausprägung im Anwenderbetrieb.

Mit der Transaktion "SU01" können neue Benutzer im SAP-System angelegt werden. Die eigentliche Vergabe der Rollen an den DSB-Benutzer ist einfach, da die Rollen für die verschiedenen Anforderungen konzipiert wurden.

⁶Das SAP ERP wird mit vier Standardbenutzern ausgeliefert: SAP*, SAPCPIP, DDIC und EARLYWATCH. Diese dienen z.B. der Installation oder Wartung, und haben Standardkennwörter. Wenn die Standardkennwörter nicht geändert wurden, ermöglicht dies einen einfachen und umfangreichen Zugang zum System.

⁷Nur in Zusammenhang mit dem Wert "Anzeigen" für das Berechtigungsobjekt "S_DEVELOP" getestet.

Damit einem Benutzer die gewünschte Berechtigungsrolle zugeordnet werden kann, wird ein Profil zu dieser Rolle mit dem Profilgenerator erzeugt. Die im verwendeten Testsystem aus den Berechtigungsrollen generierten Profile sind folgendermaßen benannt:

Z-DSB-DIS_ (Profil zur Rolle Z_AUDITOR_DSB_DIS_A)

Z-DSB-HR-D (Profil zur Rolle Z_AUDITOR_DSB_HR_DIS_A)

Z-DSB-ALL_ (Profil zur Rolle Z_AUDITOR_DSB_ALL_A).

Nachdem die Rollen vergeben wurden, sollte ein Benutzerabgleich in der Rolle durchgeführt werden.

Abschließend sind die Musterbenutzer und die ihnen zugeordneten Rollen dokumentiert.

DSB_DIS mit den Rollen:

- Z_AUDITOR_DSB_DIS
- Z_AUDITOR_DSB_DIS_A.

DSB_HR_DIS mit den Rollen:

- Z_AUDITOR_DSB_HR_DIS
- Z_AUDITOR_DSB_DIS_A
- Z_AUDITOR_DSB_HR_DIS_A.

DSB_ALL mit den Rollen:

- Z_AUDITOR_DSB_ALL
- Z_AUDITOR_DSB_DIS_A
- Z_AUDITOR_DSB_HR_DIS_A
- Z_AUDITOR_DSB_ALL_A.

A Dokumentation der entwickelten Rollen

A.1 Transaktionsrolle Z_AUDITOR_DSB_DIS

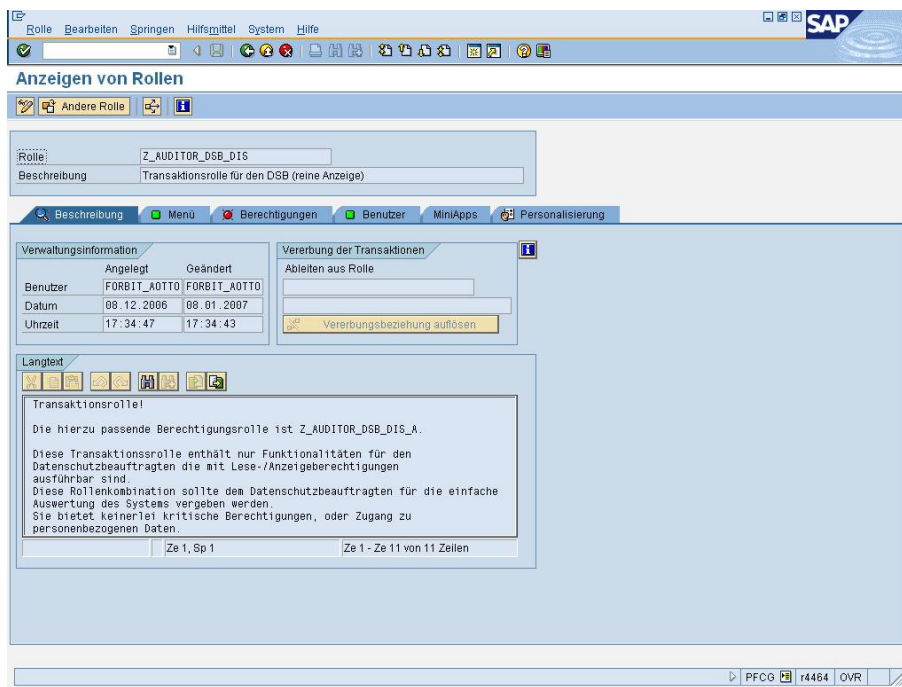


Abbildung A.1: Beschreibung der Transaktionsrolle Z_AUDITOR_DSB_DIS, Screenshot aus SAP ERP vom 08.01.2007.

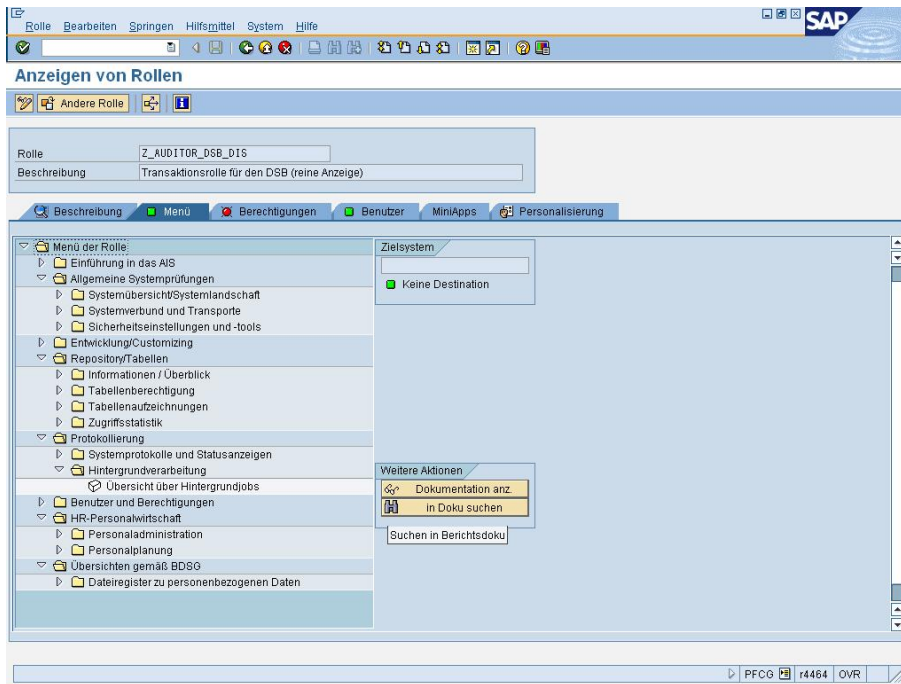


Abbildung A.2: Benutzermenü der Transaktionsrolle Z_AUDITOR_DSB_DIS (Überblick), Screenshot aus SAP ERP vom 08.01.2007.

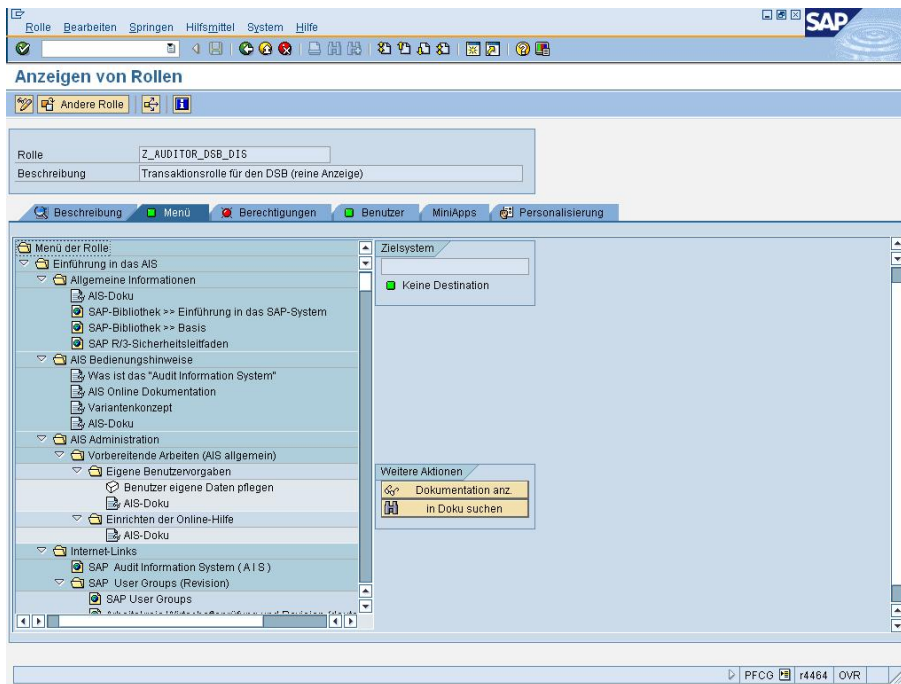


Abbildung A.3: Benutzermenü der Transaktionsrolle Z_AUDITOR_DSB_DIS, Screenshot aus SAP ERP vom 08.01.2007.

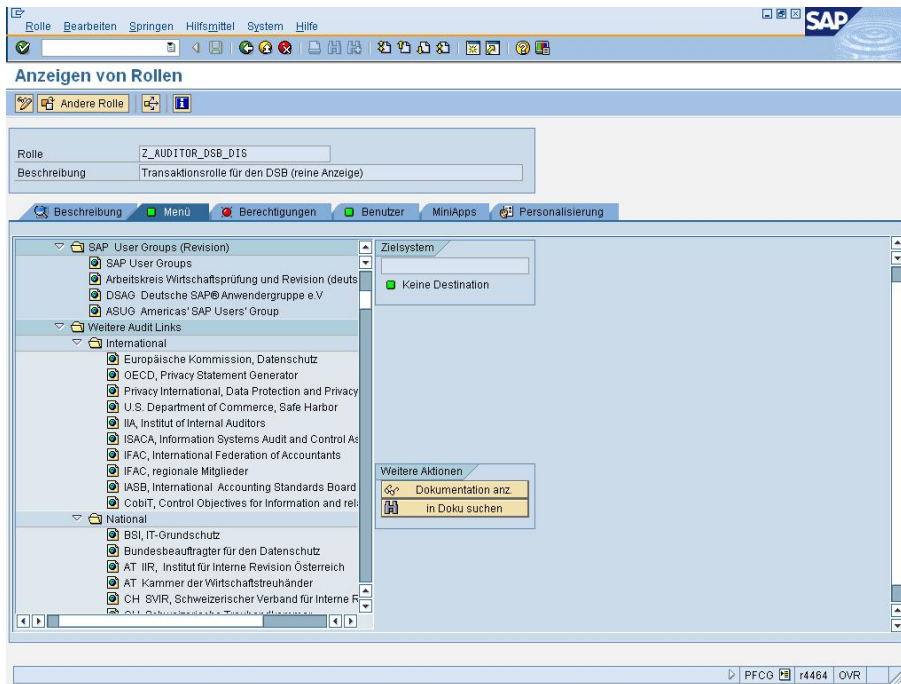


Abbildung A.4: Benutzermenü der Transaktionsrolle Z_AUDITOR_DSB_DIS, Screenshot aus SAP ERP vom 08.01.2007.

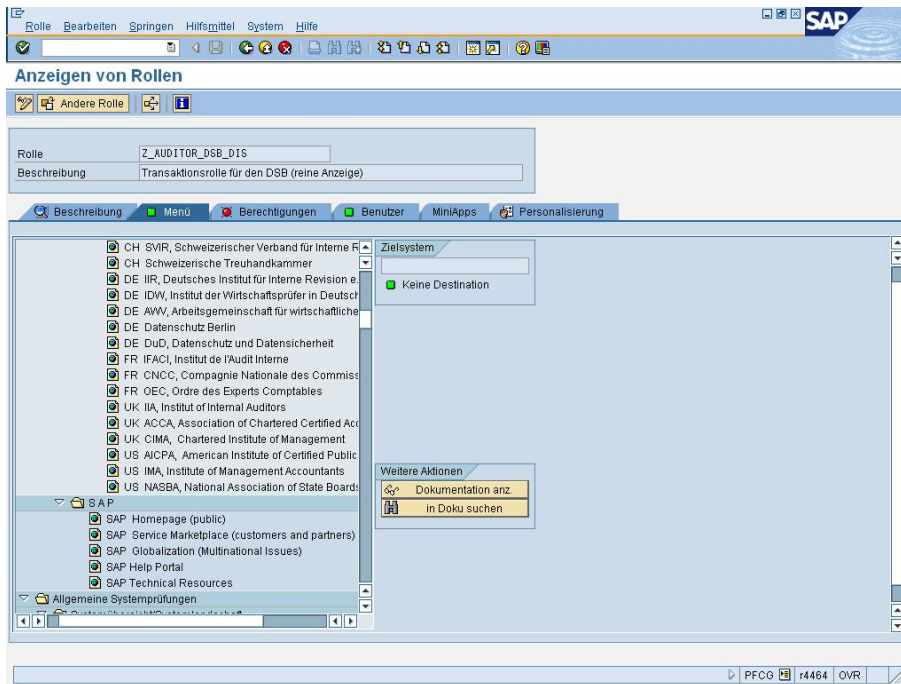


Abbildung A.5: Benutzermenü der Transaktionsrolle Z_AUDITOR_DSB_DIS, Screenshot aus SAP ERP vom 08.01.2007.

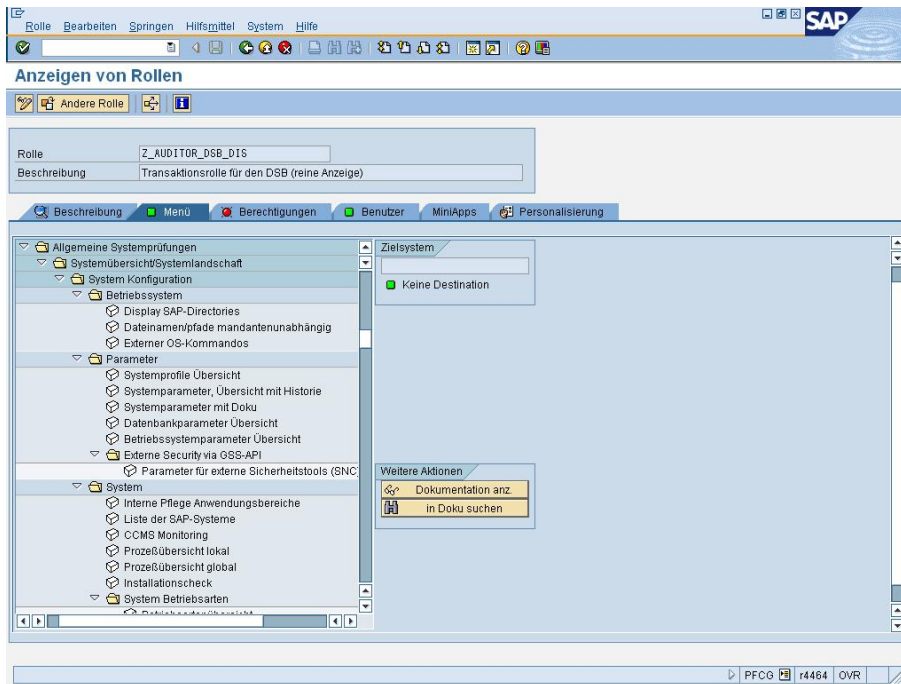


Abbildung A.6: Benutzermenü der Transaktionsrolle Z_AUDITOR_D6B_DIS, Screenshot aus SAP ERP vom 08.01.2007.

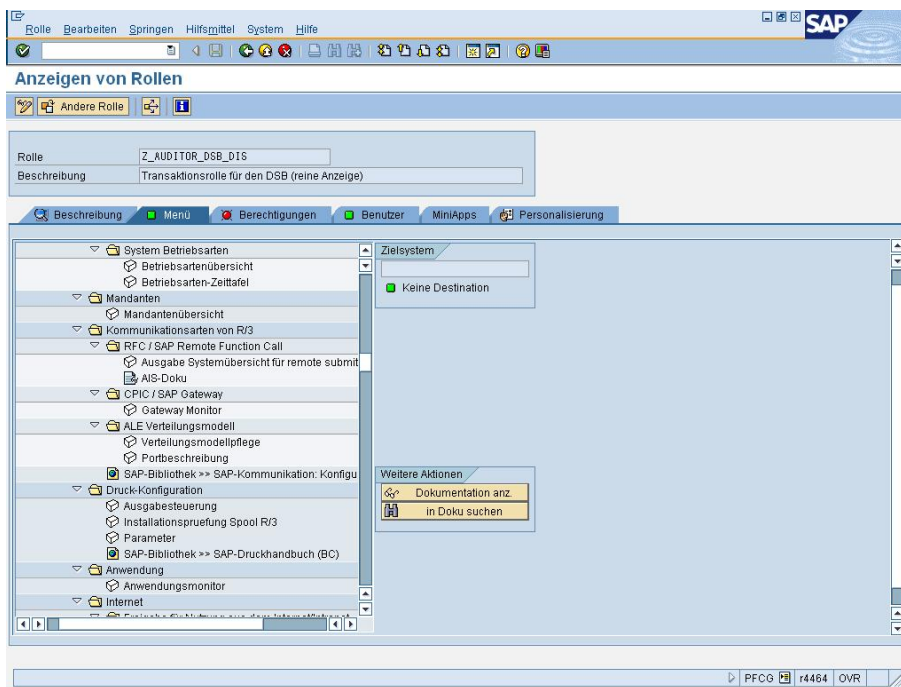


Abbildung A.7: Benutzermenü der Transaktionsrolle Z_AUDITOR_D6B_DIS, Screenshot aus SAP ERP vom 08.01.2007.

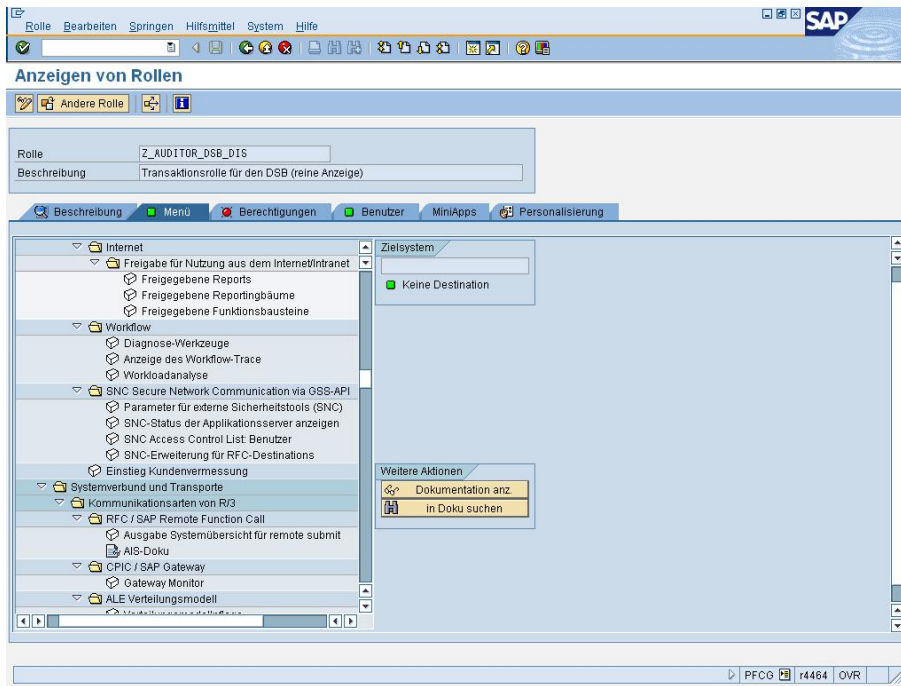


Abbildung A.8: Benutzermenü der Transaktionsrolle Z_AUDITOR_D6B_DIS, Screenshot aus SAP ERP vom 08.01.2007.

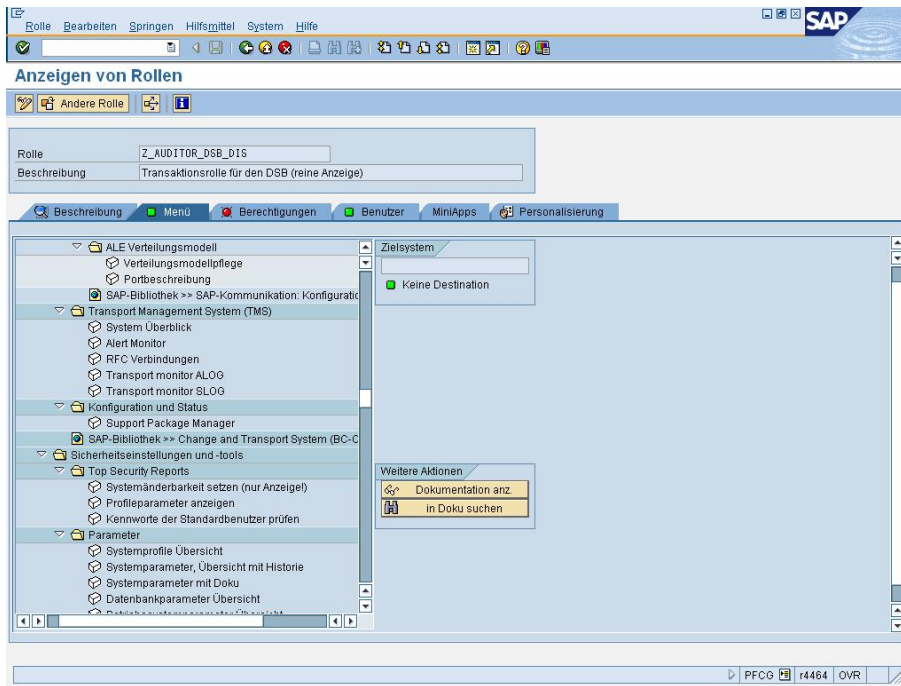


Abbildung A.9: Benutzermenü der Transaktionsrolle Z_AUDITOR_D6B_DIS, Screenshot aus SAP ERP vom 08.01.2007.

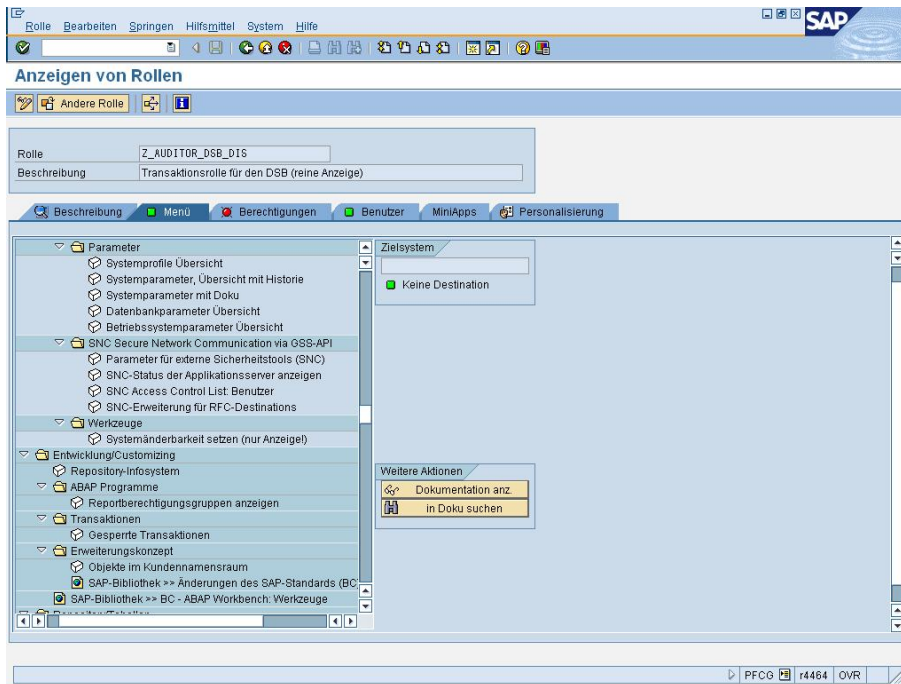


Abbildung A.10: Benutzermenü der Transaktionsrolle Z_AUDITOR_D6B_DIS, Screenshot aus SAP ERP vom 08.01.2007.

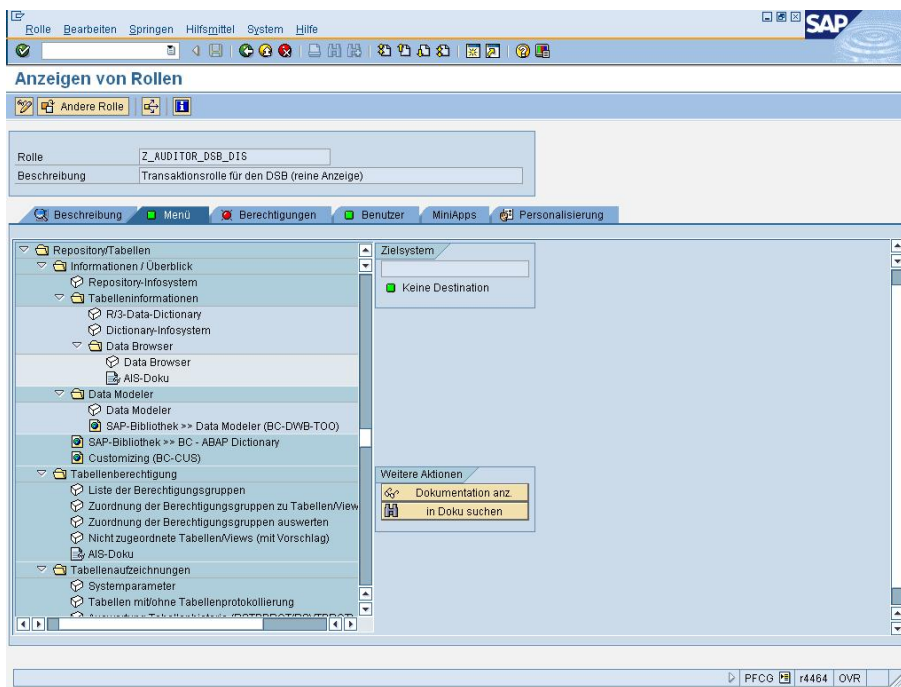


Abbildung A.11: Benutzermenü der Transaktionsrolle Z_AUDITOR_D6B_DIS, Screenshot aus SAP ERP vom 08.01.2007.

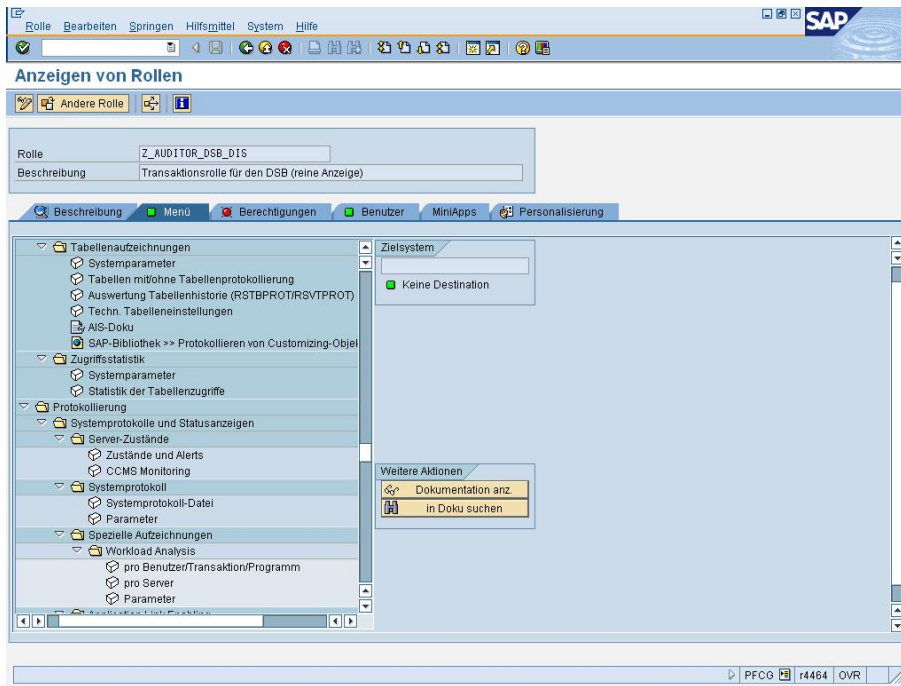


Abbildung A.12: Benutzermenü der Transaktionsrolle Z_AUDITOR_DSB_DIS, Screenshot aus SAP ERP vom 08.01.2007.

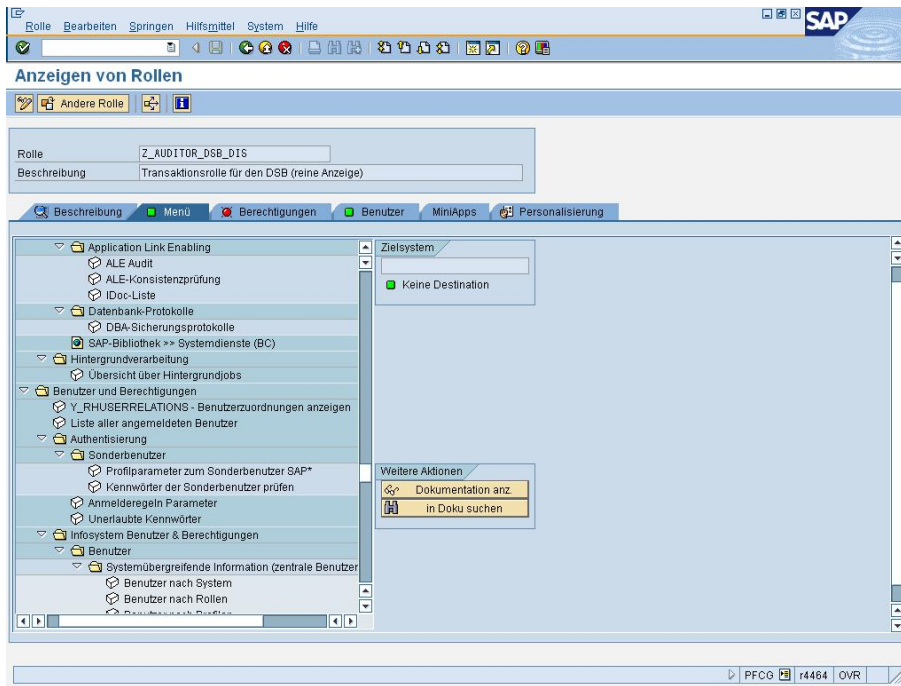


Abbildung A.13: Benutzermenü der Transaktionsrolle Z_AUDITOR_DSB_DIS, Screenshot aus SAP ERP vom 08.01.2007.

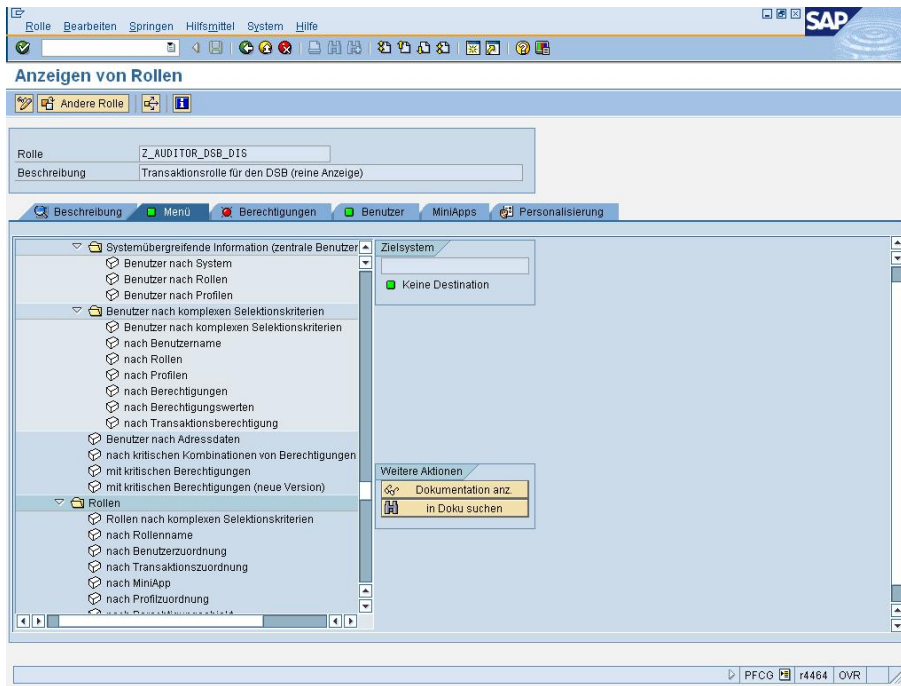


Abbildung A.14: Benutzermenü der Transaktionsrolle Z_AUDITOR_DSB_DIS, Screenshot aus SAP ERP vom 08.01.2007.

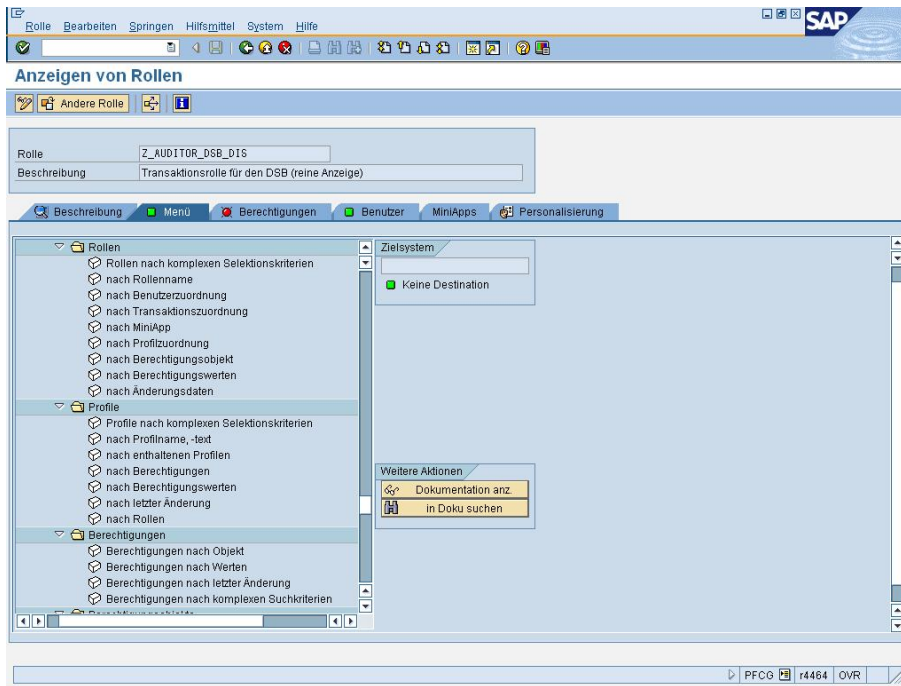


Abbildung A.15: Benutzermenü der Transaktionsrolle Z_AUDITOR_DSB_DIS, Screenshot aus SAP ERP vom 08.01.2007.

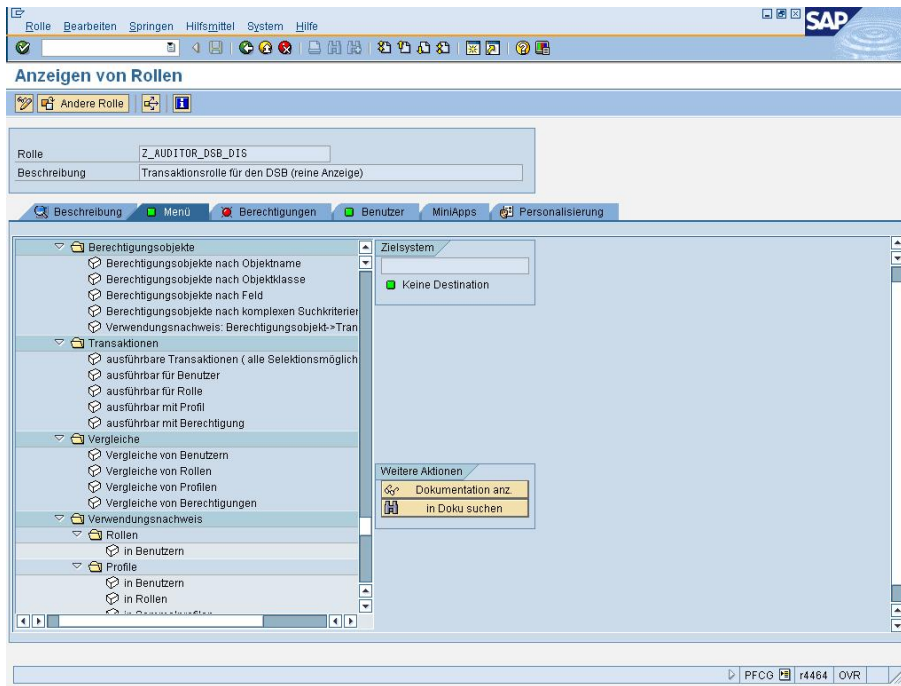


Abbildung A.16: Benutzermenü der Transaktionsrolle Z_AUDITOR_DSB_DIS, Screenshot aus SAP ERP vom 08.01.2007.

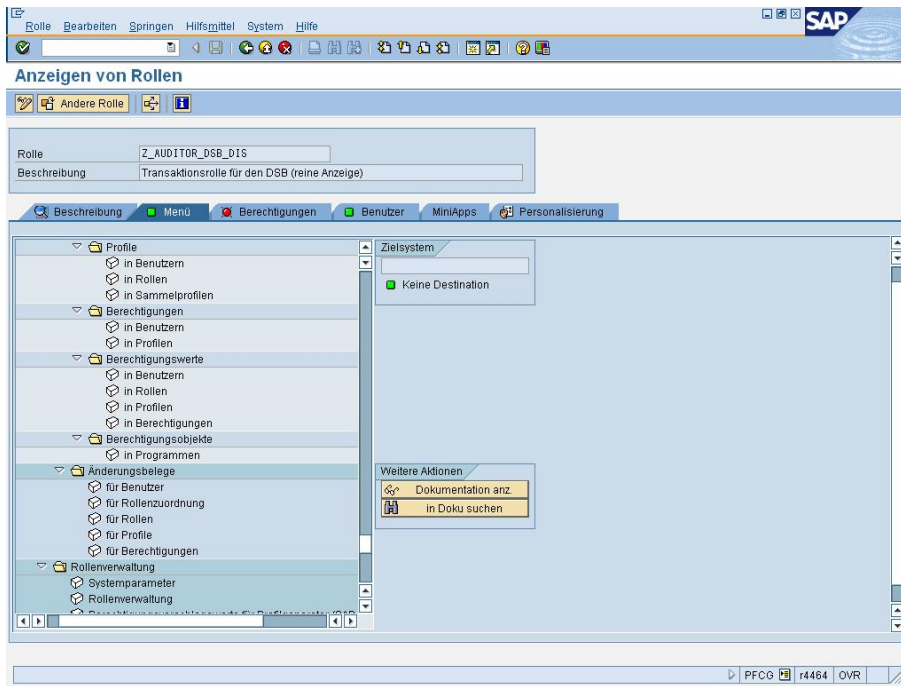


Abbildung A.17: Benutzermenü der Transaktionsrolle Z_AUDITOR_DSB_DIS, Screenshot aus SAP ERP vom 08.01.2007.

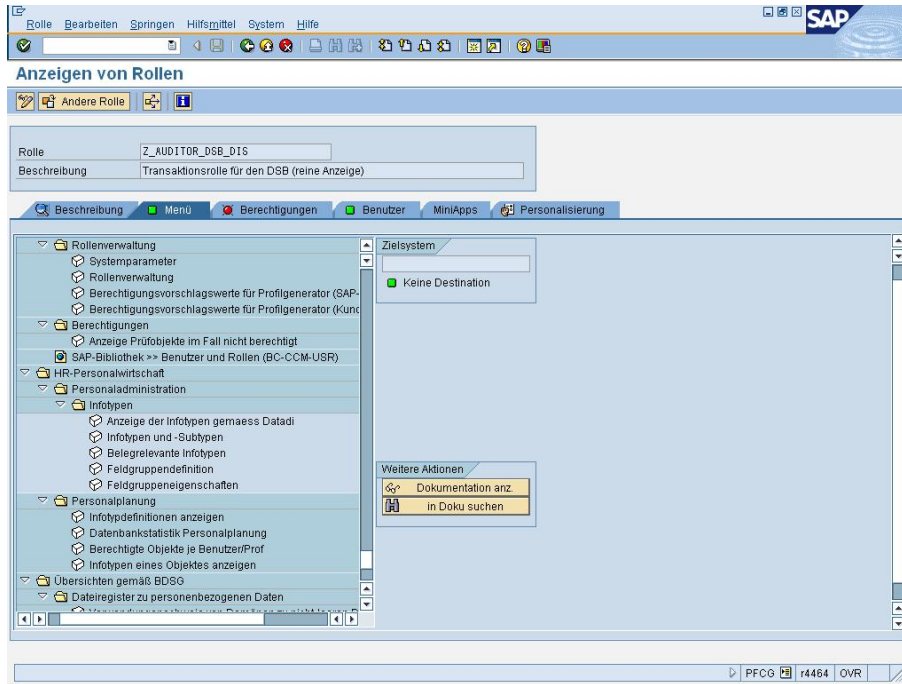


Abbildung A.18: Benutzermenü der Transaktionsrolle Z_AUDITOR_DSB_DIS, Screenshot aus SAP ERP vom 08.01.2007.

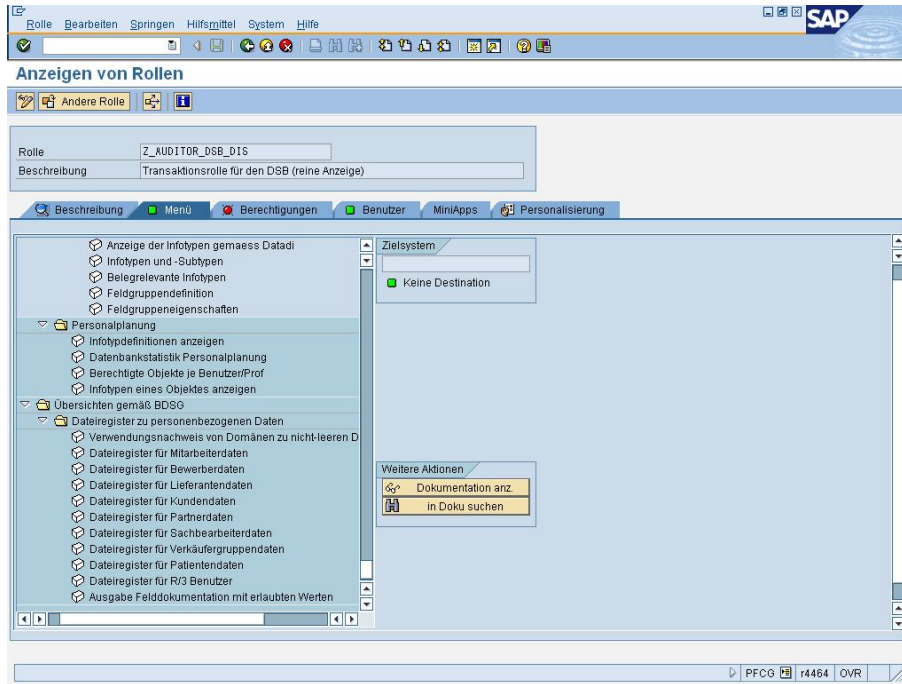


Abbildung A.19: Benutzermenü der Transaktionsrolle Z_AUDITOR_DSB_DIS, Screenshot aus SAP ERP vom 08.01.2007.

A.2 Transaktionsrolle Z_AUDITOR_DSB_HR_DIS

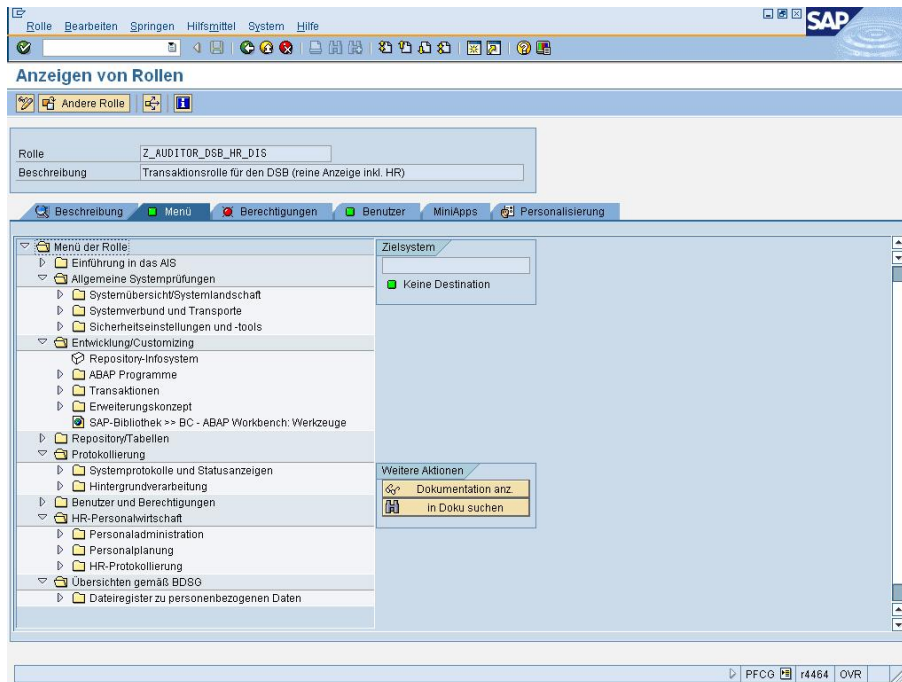


Abbildung A.20: Benutzermenü der Transaktionsrolle Z_AUDITOR_DSB_HR_DIS (Überblick), Screenshot aus SAP ERP vom 08.01.2007.

A.3 Transaktionsrolle Z_AUDITOR_DSB_ALL

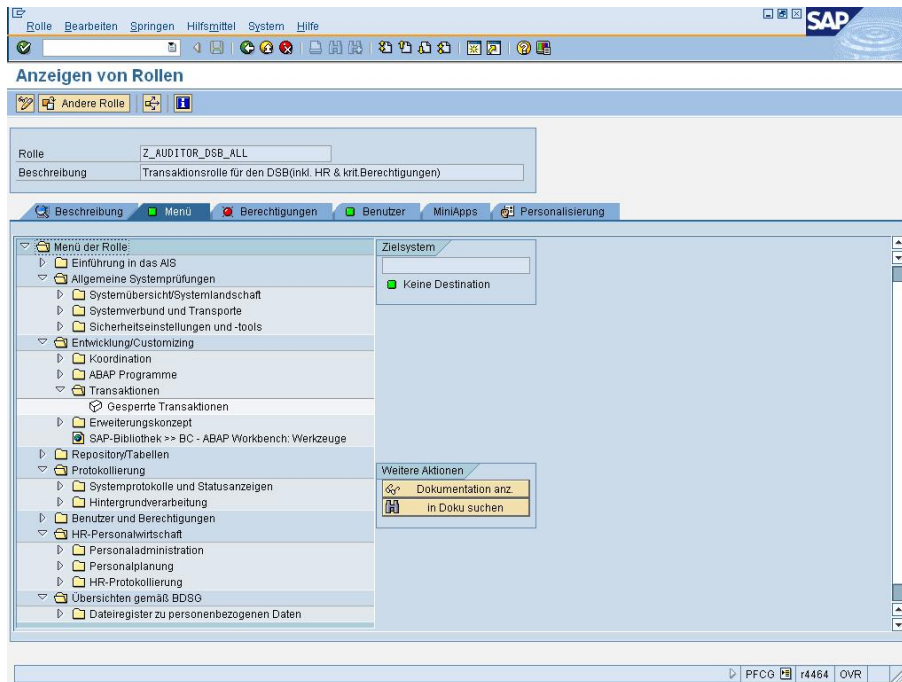


Abbildung A.21: Benutzermenü der Transaktionsrolle Z_AUDITOR_DSB_ALL (Überblick), Screenshot aus SAP ERP vom 08.01.2007.

A.4 Berechtigungsrolle Z_AUDITOR_DSB_DIS_A

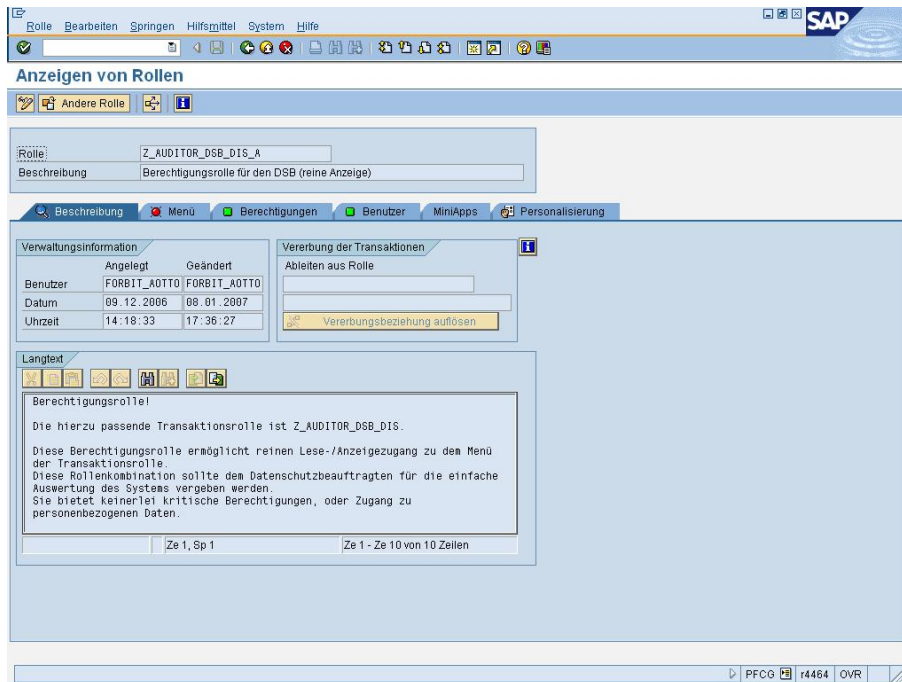


Abbildung A.22: Beschreibung der Berechtigungsrolle Z_AUDITOR_DSB_DIS_A, Screenshot aus SAP ERP vom 08.01.2007.

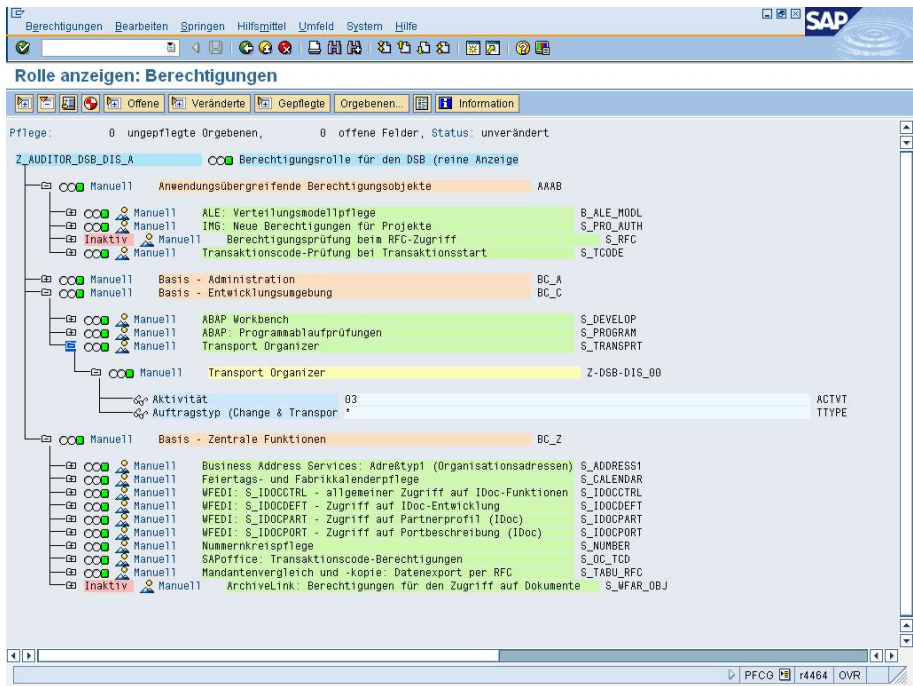


Abbildung A.23: Berechtigungen der Berechtigungsrolle Z_AUDITOR_DSB_DIS_A (Überblick), Screenshot aus SAP ERP vom 08.01.2007.

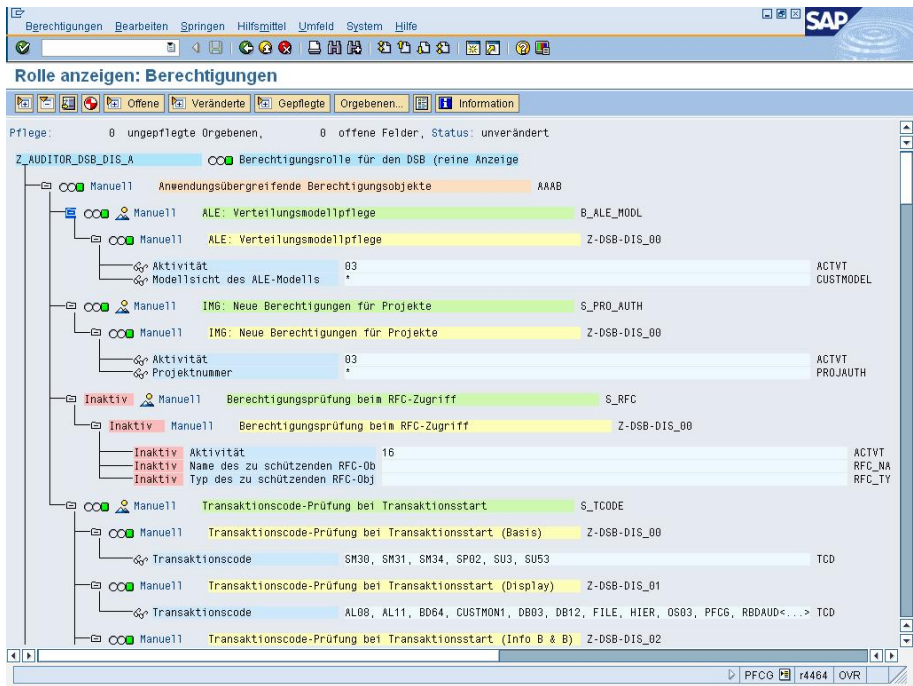


Abbildung A.24: Berechtigungen der Berechtigungsrolle Z_AUDITOR_DSB_DIS_A, Screenshot aus SAP ERP vom 08.01.2007.

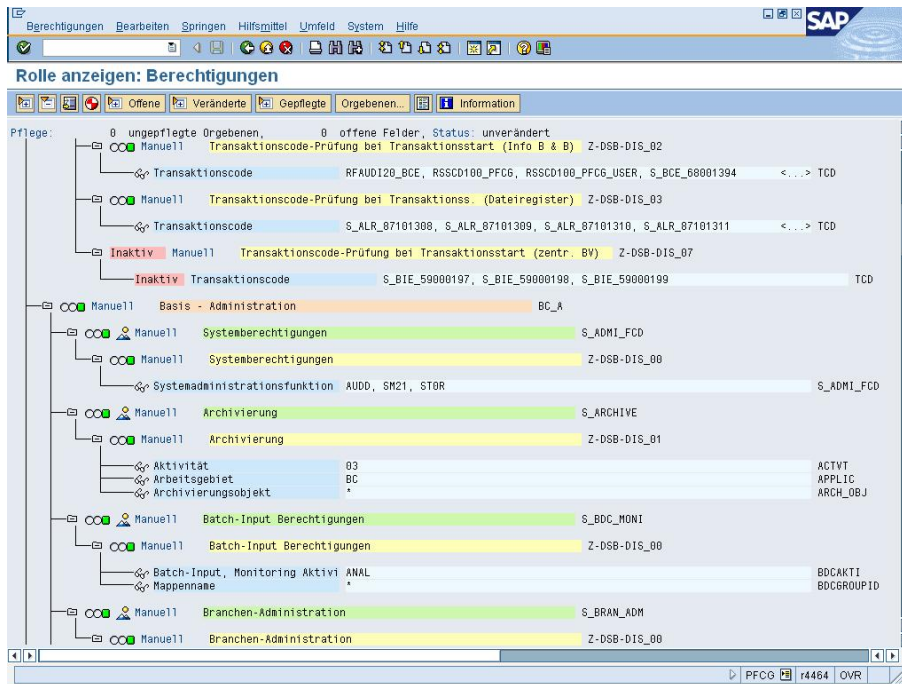


Abbildung A.25: Berechtigungen der Berechtigungsrolle Z_AUDITOR_DSB_DIS_A, Screenshot aus SAP ERP vom 08.01.2007.

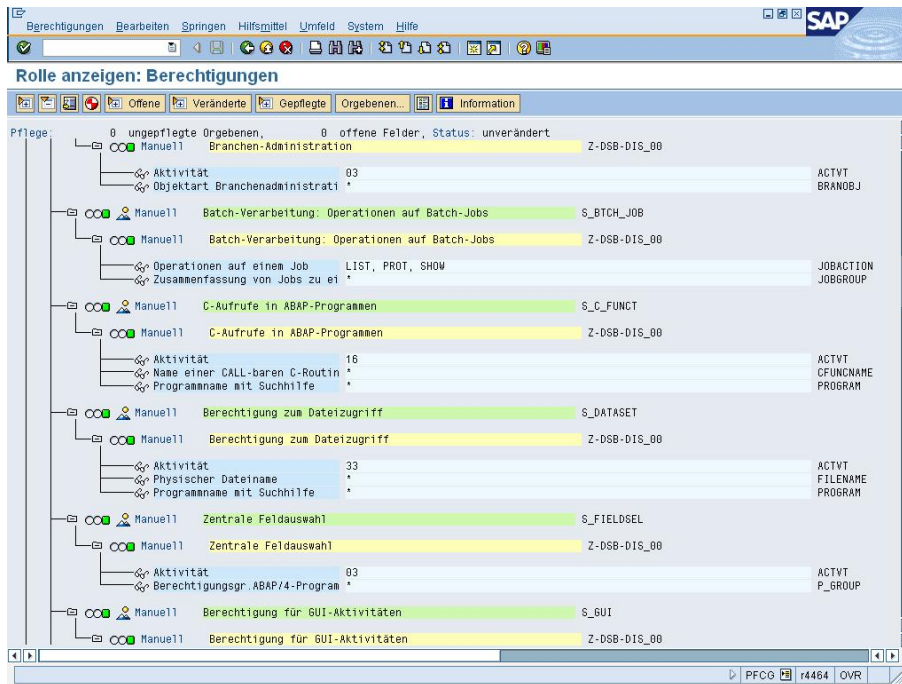


Abbildung A.26: Berechtigungen der Berechtigungsrolle Z_AUDITOR_DSB_DIS_A, Screenshot aus SAP ERP vom 08.01.2007.

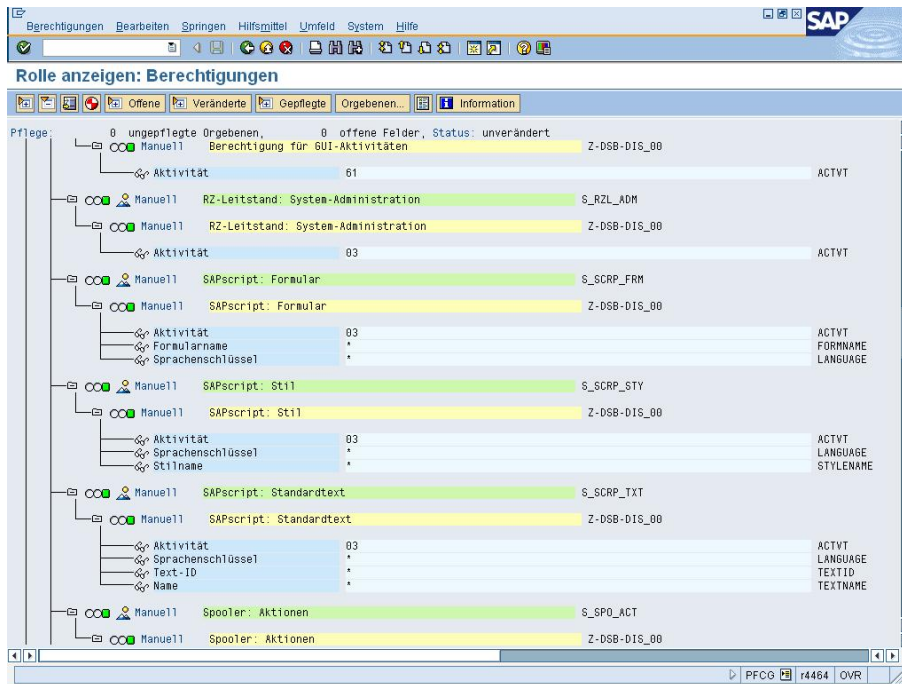


Abbildung A.27: Berechtigungen der Berechtigungsrolle Z_AUDITOR_DSB_DIS_A, Screenshot aus SAP ERP vom 08.01.2007.

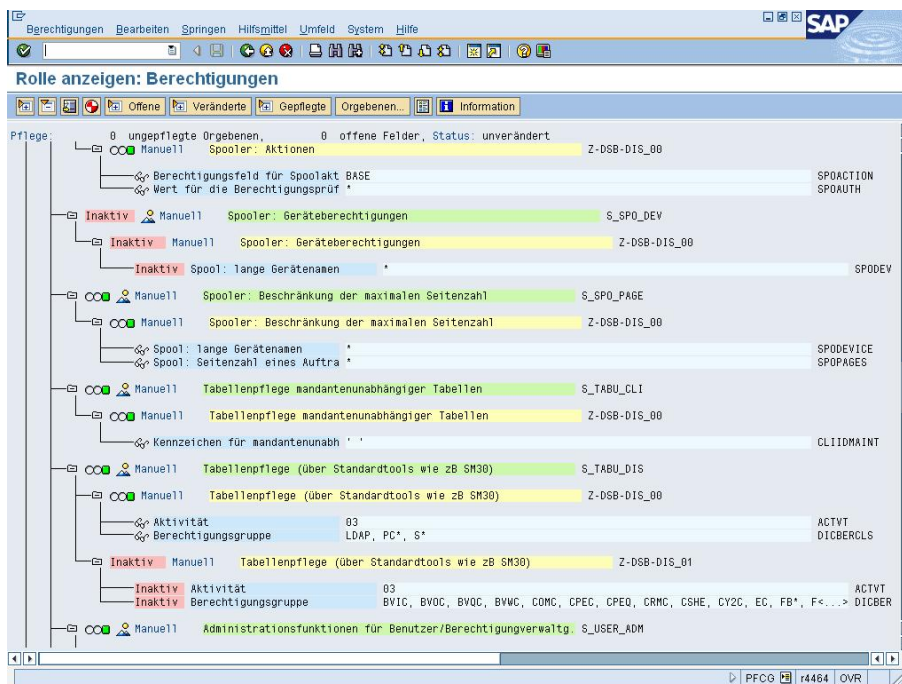


Abbildung A.28: Berechtigungen der Berechtigungsrolle Z_AUDITOR_DSB_DIS_A, Screenshot aus SAP ERP vom 08.01.2007.

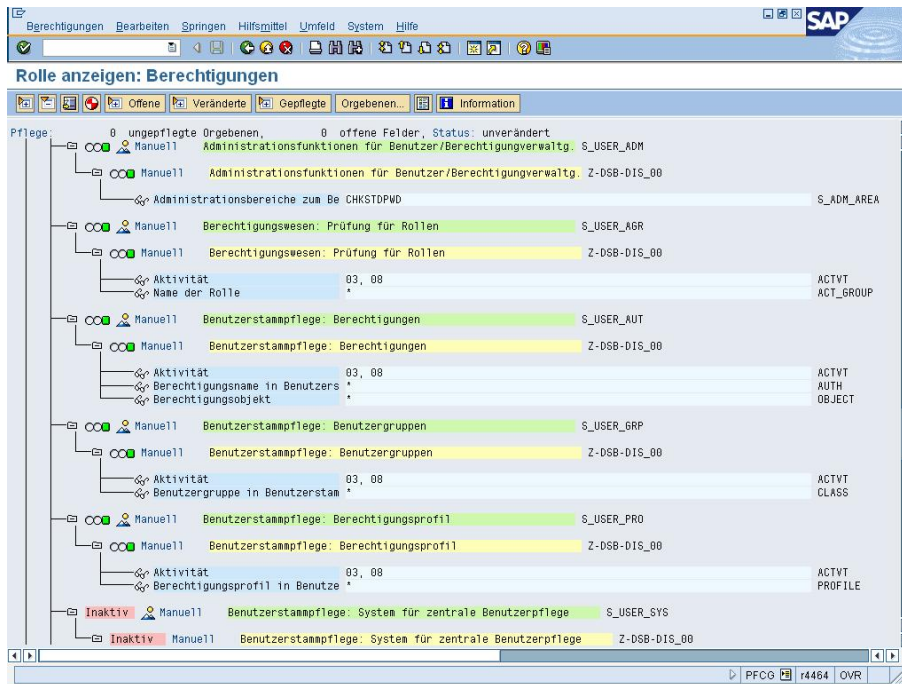


Abbildung A.29: Berechtigungen der Berechtigungsrolle Z_AUDITOR_DSB_DIS_A, Screenshot aus SAP ERP vom 08.01.2007.

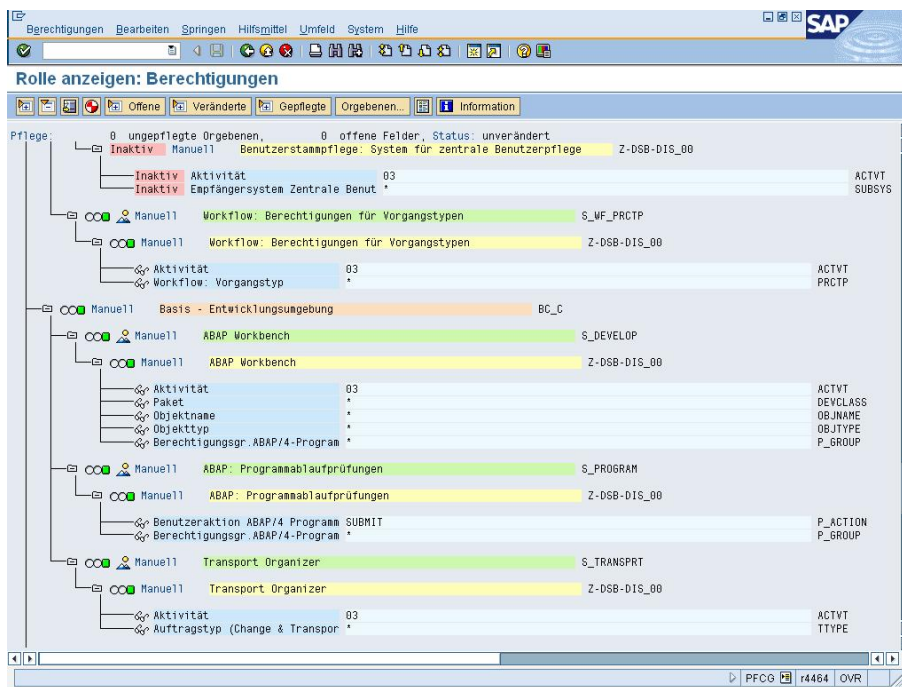


Abbildung A.30: Berechtigungen der Berechtigungsrolle Z_AUDITOR_DSB_DIS_A, Screenshot aus SAP ERP vom 08.01.2007.

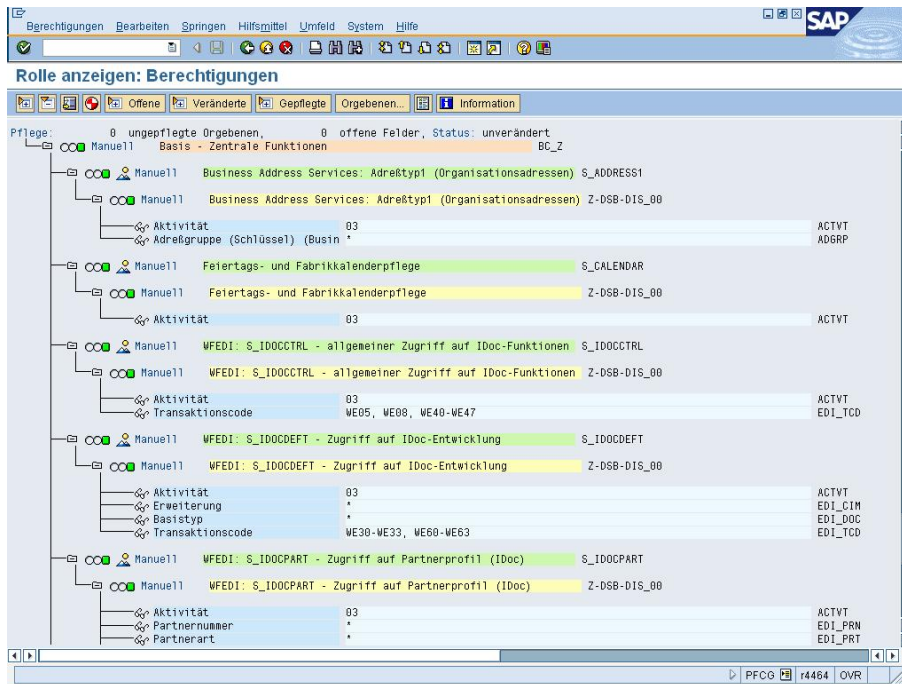


Abbildung A.31: Berechtigungen der Berechtigungsrolle Z_AUDITOR_DSB_DIS_A, Screenshot aus SAP ERP vom 08.01.2007.

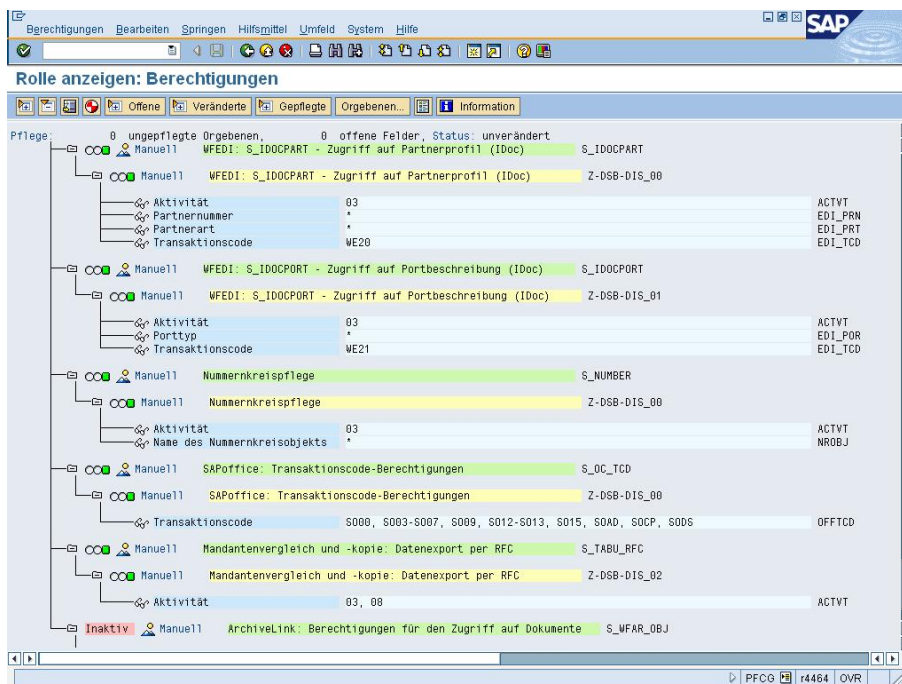


Abbildung A.32: Berechtigungen der Berechtigungsrolle Z_AUDITOR_DSB_DIS_A, Screenshot aus SAP ERP vom 08.01.2007.

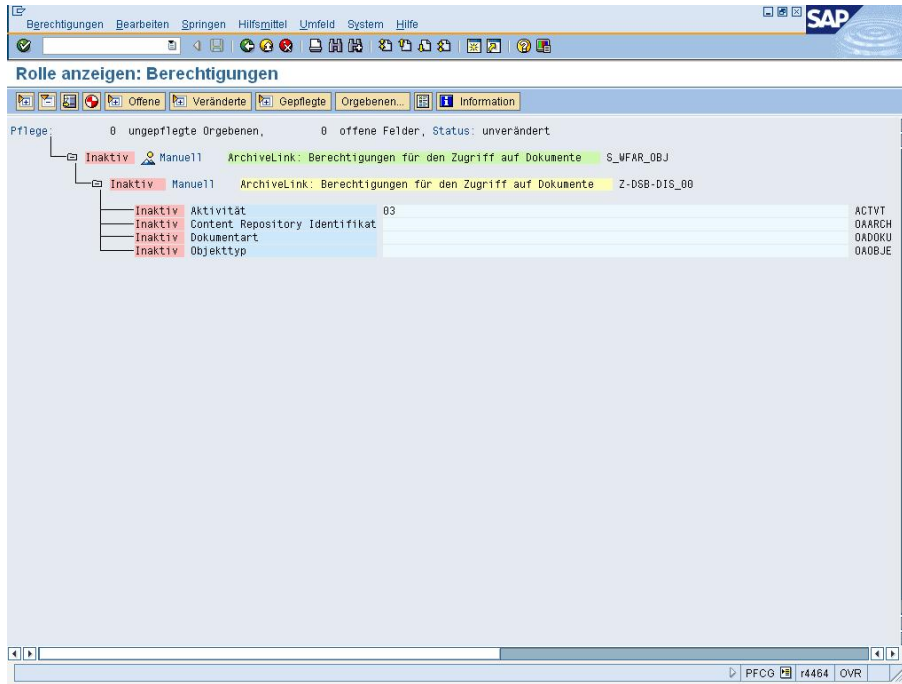


Abbildung A.33: Berechtigungen der Berechtigungsrolle Z_AUDITOR_DSB_DIS_A, Screenshot aus SAP ERP vom 08.01.2007.

A.5 Berechtigungsrolle Z_AUDITOR_DSB_HR_DIS_A

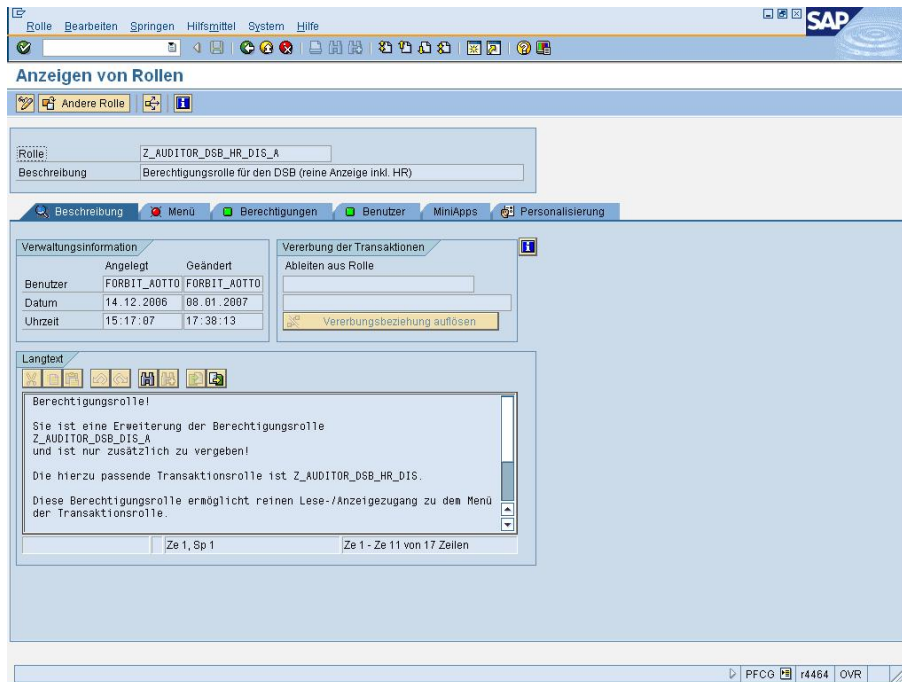


Abbildung A.34: Beschreibung der Berechtigungsrolle Z_AUDITOR_DSB_HR_DIS_A, Screenshot aus SAP ERP vom 08.01.2007.

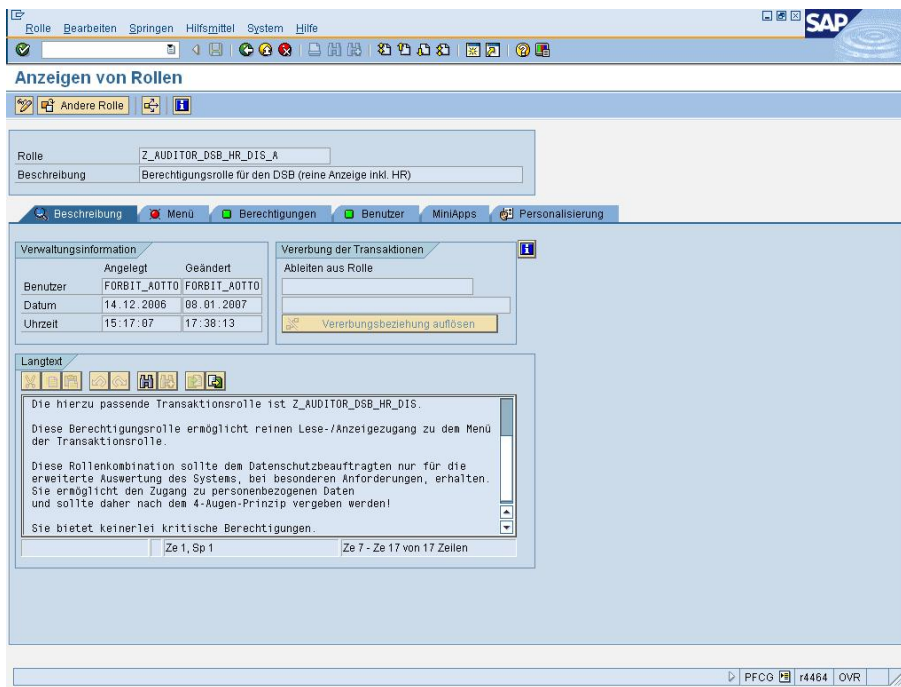


Abbildung A.35: Beschreibung der Berechtigungsrolle Z_AUDITOR_DSB_HR_DIS_A, Screenshot aus SAP ERP vom 08.01.2007.

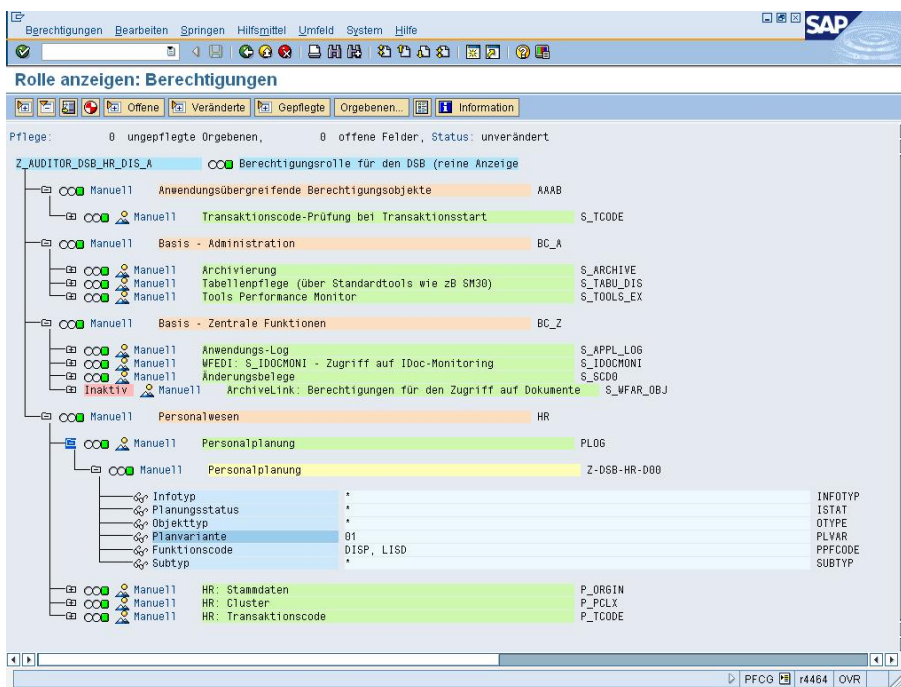


Abbildung A.36: Berechtigungen der Berechtigungsrolle Z_AUDITOR_DSB_HR_DIS_A (Überblick), Screenshot aus SAP ERP vom 08.01.2007.

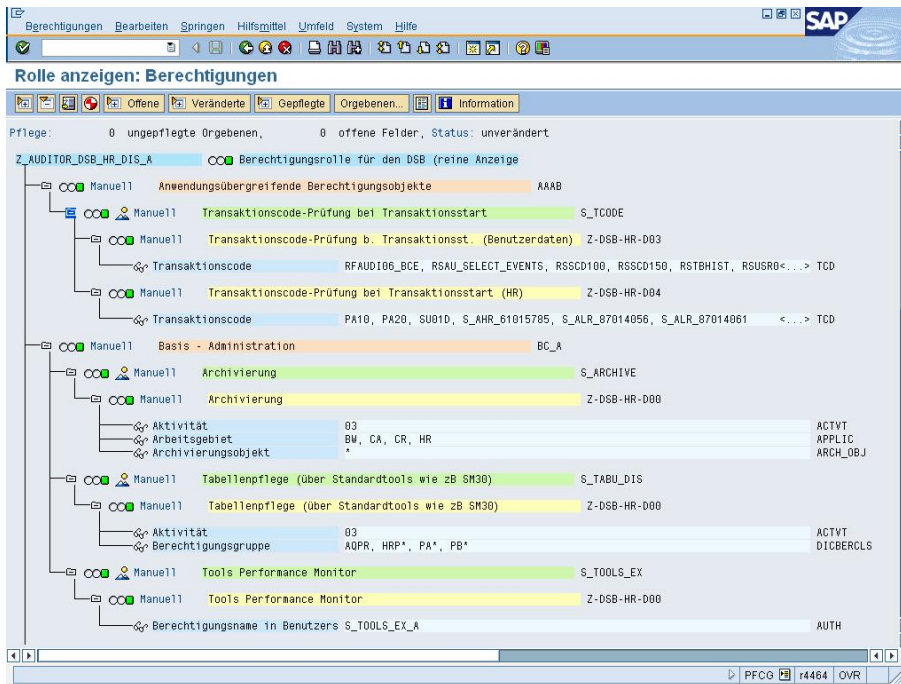


Abbildung A.37: Berechtigungen der Berechtigungsrolle Z_AUDITOR_DSB_HR_DIS_A, Screenshot aus SAP ERP vom 08.01.2007.

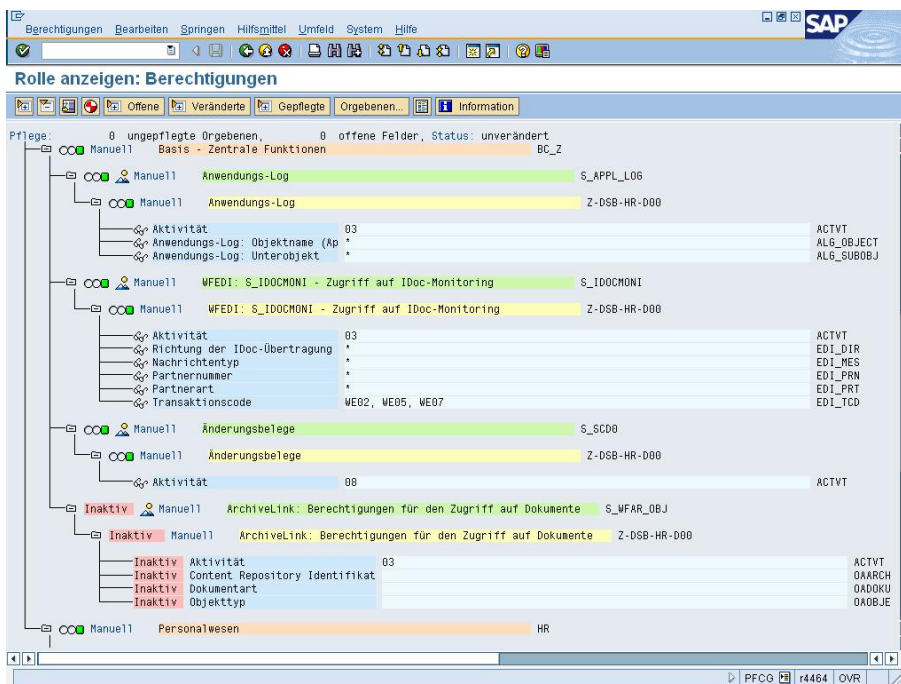


Abbildung A.38: Berechtigungen der Berechtigungsrolle Z_AUDITOR_DSB_HR_DIS_A, Screenshot aus SAP ERP vom 08.01.2007.

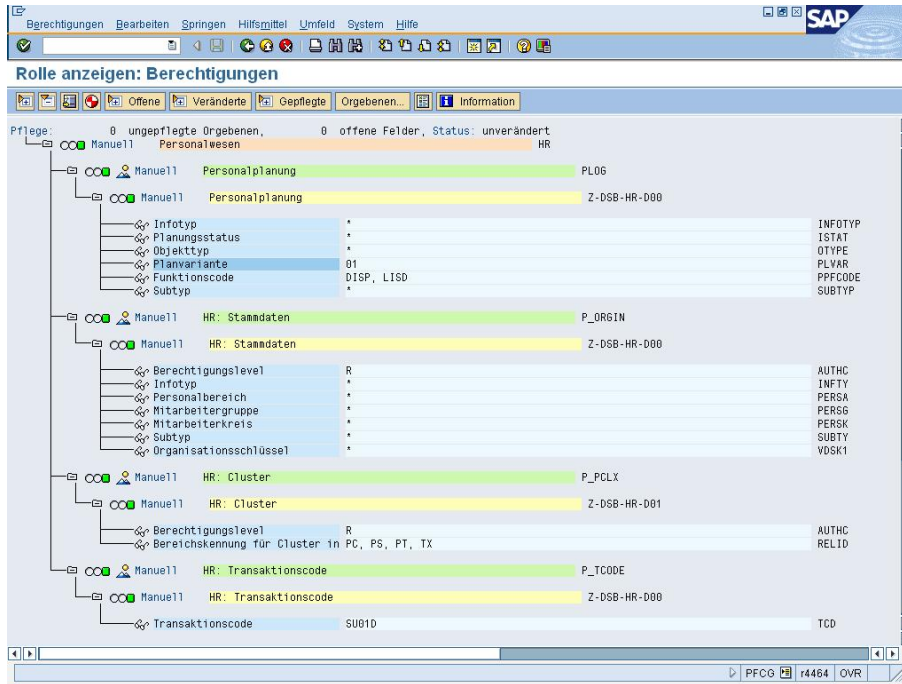


Abbildung A.39: Berechtigungen der Berechtigungsrolle Z_AUDITOR_DSB_HR_DIS_A, Screenshot aus SAP ERP vom 08.01.2007.

A.6 Berechtigungsrolle Z_AUDITOR_DSB_ALL_A

The screenshot shows the SAP ERP interface for role configuration. The title bar includes 'Rolle', 'Bearbeiten', 'Springen', 'Hilfsmittel', 'System', and 'Hilfe'. The main window is titled 'Anzeigen von Rollen' and contains the following sections:

- Rolle:** Z_AUDITOR_DSB_ALL_A
- Beschreibung:** Berechtigungsrolle für den DSB(inkl.HR & krit.Berechtigungen)
- Verwaltungsinformation:**

	Angelegt	Geändert
Benutzer	FORBIT_AOTTO	FORBIT_AOTTO
Datum	14.12.2006	08.01.2007
Uhrzeit	15:02:27	17:40:00
- Vererbung der Transaktionen:** Ableiten aus Rolle (input field), Vererbungsbeziehung auflösen (button)
- Langtext:**

Berechtigungsrolle!

Sie ist eine Erweiterung der Berechtigungsrollen Z_AUDITOR_DSB_DIS_A und Z_AUDITOR_DSB_HR_DIS_A und ist nur zusätzlich zu vergeben!

Die hierzu passende Transaktionsrolle ist Z_AUDITOR_DSB_ALL.

Diese Berechtigungsrolle bietet alle Funktionalitäten zu dem Menü der Transaktionsrolle, inklusive solcher die nur mit kritischen

Ze 1, Sp 1 Ze 1 - Ze 11 von 18 Zeilen

The status bar at the bottom shows 'PFC0', '14464', and 'OVR'.

Abbildung A.40: Beschreibung der Berechtigungsrolle Z_AUDITOR_DSB_ALL_A, Screenshot aus SAP ERP vom 08.01.2007.

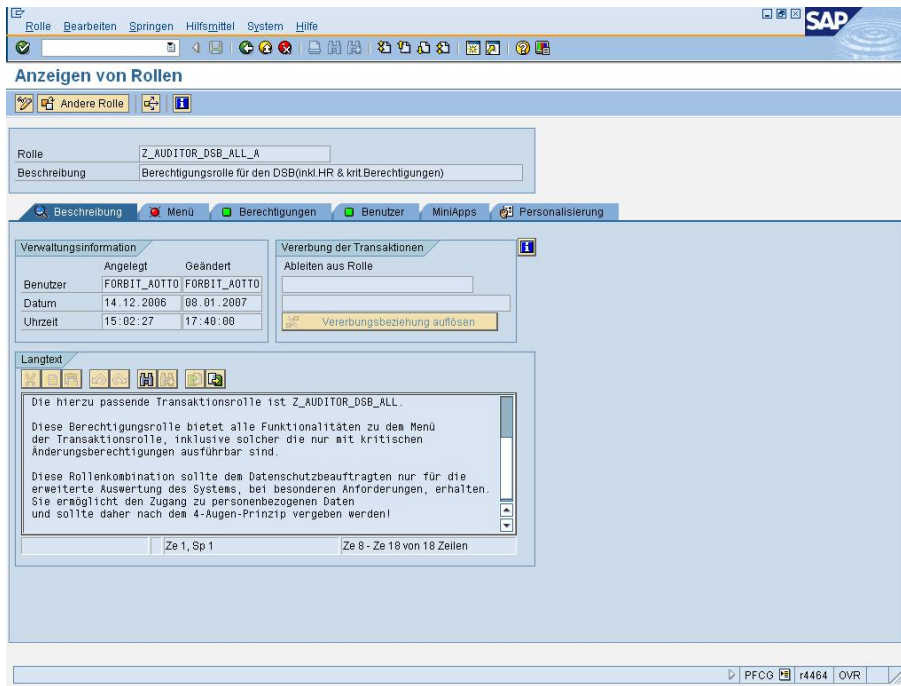


Abbildung A.41: Beschreibung der Berechtigungsrolle Z_AUDITOR_DSB_ALL_A, Screenshot aus SAP ERP vom 08.01.2007.

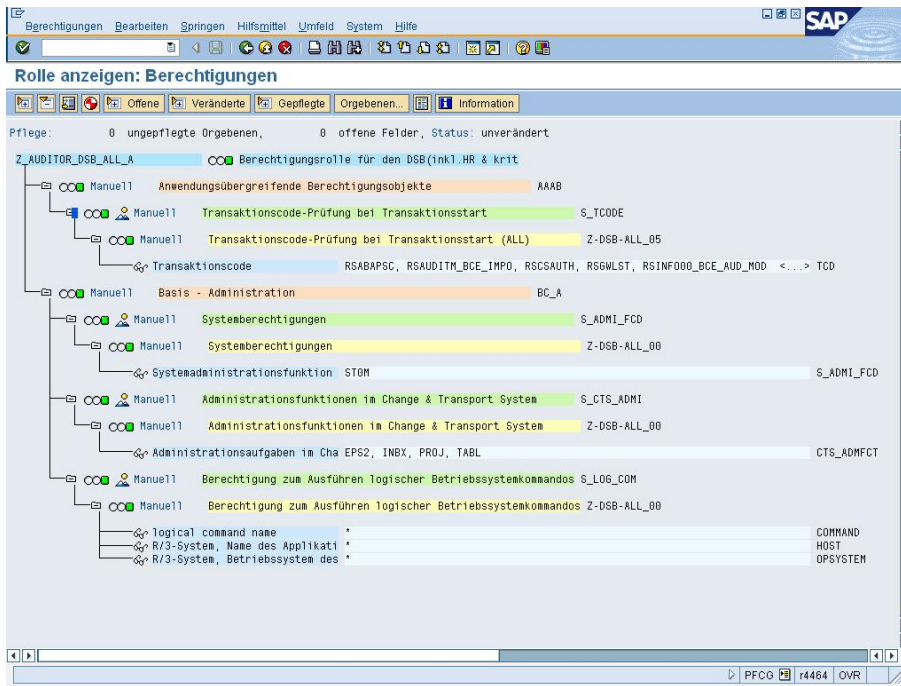


Abbildung A.42: Berechtigungen der Berechtigungsrolle Z_AUDITOR_DSB_ALL_A, Screenshot aus SAP ERP vom 08.01.2007.

B Transaktionen der entwickelten Berechtigungsrollen

Berechtigungsrolle	enthaltene Transaktionen
Z_AUDITOR_DSB _DIS_A	<p>Basis:</p> <ul style="list-style-type: none"> • SM30 • SM34 • SU3 • SM31 • SP02 • SU53 <p>Datenschutz:</p> <ul style="list-style-type: none"> • AL08 • S_ALR_87101309 • S_ALR_87101311 • S_ALR_87101313 • S_ALR_87101315 • S_ALR_87101317 • S_ALR_87101308 • S_ALR_87101310 • S_ALR_87101312 • S_ALR_87101314 • S_ALR_87101316 • S_ALR_87101318 <p>Infosystem Benutzer & Berechtigungen:</p> <ul style="list-style-type: none"> • RFAUDI20_BCE • RSSCD100_PFCG_USER • S_BCE_68001395 • S_BCE_68001397 • S_BCE_68001399 • S_BCE_68001401 • S_BCE_68001404 • S_BCE_68001406 • S_BCE_68001408 • S_BCE_68001410 • S_BCE_68001412 • S_BCE_68001414 • S_BCE_68001416 • S_BCE_68001418 • S_BCE_68001420 • S_BCE_68001422 • RSSCD100_PFCG • S_BCE_68001394 • S_BCE_68001396 • S_BCE_68001398 • S_BCE_68001400 • S_BCE_68001403 • S_BCE_68001405 • S_BCE_68001407 • S_BCE_68001409 • S_BCE_68001411 • S_BCE_68001413 • S_BCE_68001415 • S_BCE_68001417 • S_BCE_68001419 • S_BCE_68001421 • S_BCE_68001423

Tabelle B.1: Transaktionen der entwickelten Berechtigungsrollen

Berechtigungsrolle	enthaltene Transaktionen
Z_AUDITOR_DSB _DIS_A	<p>Infosystem Benutzer & Berechtigungen:</p> <ul style="list-style-type: none"> • S_BCE_68001424 • S_BCE_68001426 • S_BCE_68001428 • S_BCE_68001430 • S_BCE_68001432 • S_BCE_68001440 • S_BCE_68001767 • S_BCE_68002030 • S_BCE_68002111 • S_BCE_68001425 • S_BCE_68001427 • S_BCE_68001429 • S_BCE_68001431 • S_BCE_68001439 • S_BCE_68001441 • S_BCE_68001777 • S_BCE_68002041 • S_BIE_59000249 <p>Display:</p> <ul style="list-style-type: none"> • AL11 • CUSTMON1 • DB12 • HIER • PFCG • RBDCONCH_BCE • RDDPRCHK_AUDIT • RFTBPROT_BCE_AUDIT • RSAUDITC_BCE • RSAUDITM_BCE_TPLGA • RSEIDOC2 • RSPFPAR_LOGIN • RSPFPAR_SAPSTAR • RSPFPAR_SPOOL • RSPFPAR_SYSLOG • RSPFPAR_TABLESTAT • RSRSEDEST • RSSTAT10 • RSTMSAMO • BD64 • DB03 • FILE • OS03 • RBDAUDI01 • RDDDDATC_AUDIT_DISP • RDDTDDAT_BCE • RSABTPGP • RSAUDITM_BCE_SYSO • RSAUDITM_BCE_TPLGS • RSPFPAR • RSPFPAR_PROFGEN • RSPFPAR_SNC • RSPFPAR_STATISTICS • RSPFPAR_TABLEREC • RSPO0055 • RSSNCSRVR • RSSTAT20 • RSTMSCON_VERBOSE

Tabelle B.2: Transaktionen der entwickelten Berechtigungsrollen

Berechtigungsrolle	enthaltene Transaktionen
Z_AUDITOR_DSB _DIS_A	<p>Display:</p> <ul style="list-style-type: none"> •RSUSR003 • RZ03 • RZ10 • RZ20 • SE11 • SE15 • SE16RFC DESSECU • SE16USR40 • SE16W3 TREES • SE16WWW REPS • SE84 • SM21 • SM30V_DDAT • SM30_V_T585B • SM37 • SM51 • SM66 • SMGW • SPAM • ST10 • SWI5 • SWUD • S_ALR_87101320 • S_ALR_87101322 • S_ALR_87101324 • TU02 • WE21 •RSWBO004 • RZ04 • RZ11 • SD11 • SE13 • SE16 • SE16T000 • SE16USRACL • SE16WWW FUNC • SE17 • SICK • SM30V_BRG • SM30_V_T585A • SM30_V_T585C • SM50 • SM63 • SM69 • SP01 • ST07 • SU22 • SWU9 • S_AHR_61016267 • S_ALR_87101321 • S_ALR_87101323 • S_PH0_48000120 • USMM • Y_I10_68000200 (RHUSERRELATIONS) <hr/> <p>zentrale Benutzerverwaltung (inaktiv):</p> <ul style="list-style-type: none"> • S_BIE_59000197 • S_BIE_59000199 • S_BIE_59000198
Z_AUDITOR_DSB _HR_DIS_A	<p>Personenbezogene Daten (HR):</p> <ul style="list-style-type: none"> • PA10 • SU01D • S_ALR_87014056 • S_ALR_87014064 • PA20 • S_AHR_61015785 • S_ALR_87014061

Tabelle B.3: Transaktionen der entwickelten Berechtigungsrollen

Berechtigungsrolle	enthaltene Transaktionen
Z_AUDITOR_DSB _HR_DIS_A	Leistungsanalyse: <ul style="list-style-type: none"> ● RFAUDI06_BCE ● RSSCD100 ● RSTBHIST ● RSUSR007 ● RSUSR200_ INITPASS ● RSUSR200_ UNUSED30 ● SLG1 ● SM20N ● STAD ● S_ALR_87014082 ● RSAU_SELECT_EVENTS ● RSSCD150 ● RSUSR000 ● RSUSR200 ● RSUSR200_ PWDCHG180 ● SCU3 ● SM20 ● SM30_V_T599R ● S_ALR_87014081 ● S_BCE_68001402
Z_AUDITOR_DSB _ALL_A	All: <ul style="list-style-type: none"> ● RSABAPSC ● RSCSAUTH ● RSINFO00_BCE_ AUD_MOD ● RSPFPAR_AUTH ● RSPFPAR_RFC ● RSRFCSTX ● RSSWOUSR ● RSWBO040 ● RZ01 ● SA38 ● SARA ● SCC3 ● SCDO ● SCUM ● SE06 ● SE12 ● SM04 ● SM30 ● SM34 ● SM54 ● SM59 ● SMT2 ● SMW0 ● ST22 ● SU56 ● SWU2 ● RSAUDITM_BCE_IMPO ● RSGWLST ● RSPFPAR_ CALLSYSTEM ● RSPFPAR_GATEWAY ● RSRFCCHK ● RSRFCTRC ● RSTMSDIC ● RSWBO050 ● RZ27_SECURITY ● SAMT ● SARP ● SCDN ● SCUL ● SE03 ● SE09 ● SE16V_T599R ● SM13 ● SM30VSNCSYSACL ● SM35 ● SM58 ● SMT1 ● SMTS ● ST01 ● SU05 ● SWEL ● S_AHR_61016266

Tabelle B.4: Transaktionen der entwickelten Berechtigungsrollen