SAP R/3 – Besonderheiten des Systems bei der Prüfung des Berechtigungskonzeptes

Von Dipl.-Betriebswirt Christoph Wildensee, Hannover [1]

1. Einführung

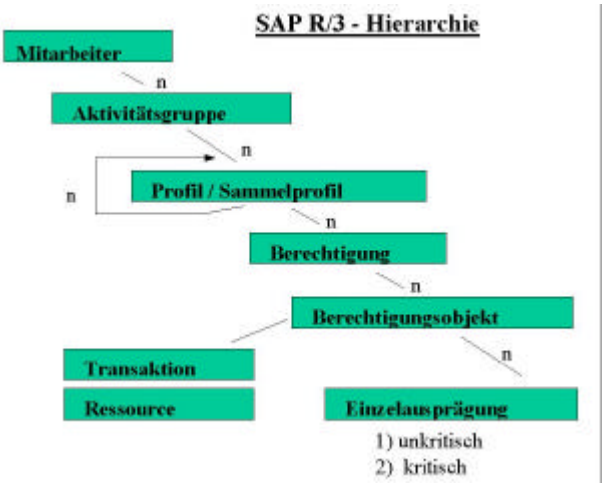
Durch die Komplexität des SAP R/3-Systems ist die Prüfung des Berechtigungskonzeptes eine zentrale und wiederkehrende Aufgabe für einen IV-Revisor. Die Systemprüfung mit dem Anspruch eines ganzheitlichen Ansatzes hinsichtlich bestehender Sicherheitsrisiken ist als einmaliger Vorgang kaum durchführbar. Man kann nur iterativ prüfen und hierbei mit unterschiedlichen, aufeinander aufbauenden Fragestellungen arbeiten. Um in angemessener Zeitvorgabe Prüfungen durchzuführen, müssen umfassende Kenntnisse über den Aufbau der Berechtigungsvergabe auf SAP-Ressourcen und / oder entsprechende Dokumentationen über die zugrundeliegenden Berechtigungsverwaltungsobjekte im schnellen Zugriff vorhanden sein.

Der nachfolgende Artikel soll in Kurzform die Berechtigungsvergabe und die damit verbundenen Problemfelder anreißen und dabei einen möglichen Bearbeitungsansatz für eine effektive Prüfungsvorbereitung liefern.

2. Das SAP R/3 - Berechtigungskonzept

Das SAP-System unterscheidet zum einen die Transaktion, die den Zugang zu SAP-Funktionalitäten abstrakt definiert und zum anderen die Berechtigungsobjekte, die - als Masken über die Transaktionen gelegt - dezidiert Einschränkungen innerhalb dieser Funktionswahrnehmung zulassen. So lassen sich also innerhalb der Vergabe auf Berechtigungsobjekte Unterscheidungen treffen hinsichtlich des Datenmanipulationsgrades (Aktivität Anzeigen, Ändern, Hinzufügen, Buchen etc.), aber auch hinsichtlich der Zugriffe auf einzelne Buchungskreise, Perioden, Nummernkreise usw. Die Berechtigungen sind durch die Einzelausprägungen der Berechtigungsobjektfelder definiert. Ein Berechtigungsobjekt kann sich nicht nur auf eine Transaktion/betriebswirtschaftliche Funktion beziehen, meistens ist es in mehreren zu finden. Ebenfalls ist es üblich, dass zum Ausführen einer Transaktion die Zugriffsdefinition auf mehrere Berechtigungsobjekte vorhanden sein muss.

Nachfolgende Grafik skizziert grob die SAP-Hierarchie innerhalb des Berechtigungskonzeptes.



Die SAP R/3-Berechtigungsvergabe ist somit das Zusammenspiel von Transaktionen und Berechtigungsobjekten, zusammengefasst in Profilen/Sammelprofilen und diese wiederum in aufgabenorientierten Rollen/Aktivitätsgruppen.

---

1 C. Wildensee ist bei der Stadtwerke Hannover AG als IV-Revisor und stellvertr. Datenschutzbeauftragter tätig.

Nicht jede Transaktion beinhaltet eine Berechtigungsprüfung. Freie Transaktionen sind jedoch nicht so umfangreich vorhanden und nicht sehr kritisch. Viele davon beziehen sich ausschließlich auf Verwaltungsobjekte des jeweiligen Nutzers (z.B. SU0x, SU3; SU5x). Keiner dieser Zugänge hat ändernde Zugriffe auf kritische Bereiche des SAP-Systems.

Der Zugriff auf die jeweiligen Transaktionen, die üblicherweise dem Benutzer zugewiesen sein müssen, wird grundsätzlich über das Berechtigungsobjekt S_TCODE mit dem Feld TCD (Transaktionscode) gewährleistet.

2.1 ABAP-Quellcode

Nahezu alle Transaktionen und sonstigen Verwaltungsfunktionen sind in ABAP geschrieben, d.h. mit der SAP-eigenen Programmiersprache, die mit einem sehr mächtigen Sprachumfang umfassende Manipulationsmechanismen innerhalb von SAP R/3 bietet. Die Orientierung an einer Sprache hat innerhalb des Berechtigungskonzeptes jedoch auch einen Nachteil. Die Ressourcen werden nicht als solche gegen unberechtigte Zugriffe abgeschirmt, vielmehr muss die Berechtigungssteuerung innerhalb der Programme mit ABAP-Funktionsaufrufen bzw. -Sprachmitteln erfolgen.
Um dieser Notwendigkeit Rechnung zu tragen, wird über das ABAP-Statement 'AUTHORITY-CHECK' - entweder direkt im Hauptcoding oder über einen Funktionsbausteinaufruf - die Prüfung auf die jeweilige SAP-Ressource durchgeführt. Dieses Statement erhält als Übergabewerte das zu prüfende Berechtigungsobjekt, die jeweiligen Steuerungsfelder des Berechtigungsobjektes und die notwendigen Feldinhalte als Zugangsvoraussetzung zu der SAP-Funktionalität. Ist der Abgleich zwischen notwendigem Zugangwert und Vergleichwert des Mitarbeiters aus seiner Zuweisung erfolgreich, wird der Wert 0 als Returncode zurückgegeben, ansonsten erfolgt über einen anderen Returncode eine Ablehnung. Innerhalb des Zugriffs auf einzelne Funktionen/Ressourcen erfolgt meist der Abgleich auf mehrere Berechtigungsobjekte, die in Gänze zutreffen müssen, um Zugriff auf die Funktionalität zu erhalten. So darf also sowohl bei der Programmierung als auch bei der Prüfung weder das Berechtigungsobjekt noch die jeweils gültige Einzelausprägung der zugehörigen Felder übergangen werden.

Beispiel:

```
AUTHORITY-CHECK OBJECT F_BKPF_GSB                 Buchhaltungsbelege-Geschäftsbereich
  ID 'ACTVT' FIELD act_hinz                       Aktivität wie Feld act_hinz
  ID 'GSBER' FIELD aut_gsber.                     Geschäftsbereich wie Feld aut_gsber
IF sy-subrc NE 0.                                 wenn fehlerhafter Abgleich dieser
 xauth-xerro = 'X'.                               Felder, dann wird in ein Feld einer
                                                  internen Tabelle xauth (Feld xerro)
ENDIF.                                            eine Kennzeichnung gesetzt = 'X'
APPEND xauth.                                     Die Kennzeichnung wird in die
                                                  interne Tabelle xauth geschrieben/
[...]                                             an diese angehängt
IF xauth-xerro NE SPACE.                          wenn das Kennzeichnungsfeld nicht
                                                  leer ist (also 'X' = 'Fehler'), dann
MESSAGE e085 WITH aut_gsber.                      Ausgabe eines Fehlers mit Bezug zum
ENDIF.                                            Geschäftsbereich aut_gsber und Neueing.
[...]                                             ansonsten weiter im Programm und
AUTHORITY-CHECK OBJECT ...                        nächster authority-check -Block
```

Innerhalb der Bereitstellung solcher Funktionalitäten erfolgt ggf. nacheinander der Aufruf mehrerer solcher AUTHORITY-CHECK-Anweisungen und entsprechender wenn-dann-Beziehungen, um innerhalb der Zugangssteuerung die negativen Ausprägungen abzufangen, bevor die eigentliche Funktionalität für den Benutzer freigegeben wird. Die Returncodeanalyse nimmt in jedem Programm eine zentrale Rolle ein, denn nur hierüber ist eine Steuerung möglich.

2.2 Tabellenprüfungen

Es gibt eine Vielzahl von Tabellen, die die Berechtigungsprüfung erleichtern. Hier werden beispielhaft sechs der wichtigsten Tabellen erläutert, die dem Revisor - ein Zugriff über die Transaktion SE16 (Data Browser: Einstieg) vorausgesetzt - umfassende Hilfestellungen geben können.

2.2.1 USOBT - Relation Transaktion -> Ber.objekt

Die Tabelle USOBT zeigt die Verbindung zwischen einer Transaktion und den zugehörigen Berechtigungsobjekten. Sie ist sehr wichtig, um zum einen diese o.g. involvierten Berechtigungsobjekte auf einen Blick zu identifizieren, und zum anderen, um auch die kritischen Ausprägungen zu erkennen.

Beispiel FB03 - Beleg anzeigen

Liste aus USOBT:

NAME	TYPE	OBJECT	FIELD	LOW	HIGH	[...]
FB03	TR	F_BKPF_BED	ACTVT			
FB03	TR	F_BKPF_BED	BRGRU			
FB03	TR	F_BKPF_BEK	ACTVT			
FB03	TR	F_BKPF_BEK	BRGRU			
FB03	TR	F_BKPF_BES	ACTVT			
FB03	TR	F_BKPF_BES	BRGRU			
FB03	TR	F_BKPF_BLA	ACTVT			
FB03	TR	F_BKPF_BLA	BRGRU			
FB03	TR	F_BKPF_BUK	ACTVT	03		
FB03	TR	F_BKPF_BUK	BUKRS	$BUKRS		
FB03	TR	F_BKPF_BUP	BRGRU			
FB03	TR	F_BKPF_GSB	ACTVT	03		
FB03	TR	F_BKPF_GSB	GSBER	$GSBER		
FB03	TR	F_BKPF_KOA	ACTVT	03		
FB03	TR	F_BKPF_KOA	KOART	$KOART		

Hier ist zu erkennen, dass zur Nutzung der Transaktion FB03 - Beleg anzeigen - der Zugriff auf mehrere Berechtigungsobjekte in einer bestimmten Konstellation der Felder vorliegen muss. Dies sind das Objekt F_BKPF_BUK mit der Vorgabe Aktivität 03 = Anzeigen und der Buchungskreiseingrenzung, weiterhin das Objekt F_BKPF_GSB mit der Aktivität 03 = Anzeigen und der Geschäftsbereichseingrenzung und zum Schluss das Objekt F_BKPF_KOA mit der Aktivität 03 = Anzeigen und der Kontoarteneingrenzung (BUKRS, GSBER und KOART abhängig von der Einrichtung des Systems, daher hier keine festen Vorgaben).

2.2.2 TSTC - SAP-Transaktions-Codes

Die Tabelle TSTC zeigt die zu den Transaktionen gehörenden Haupt-Programmnamen an. Mit diesem und der Berechtigung auf SE38 - ABAP Editor: Einstieg - kann der zum Transaktionscode gehörige Programmcode analysiert werden, beispielsweise mit der Suche nach dem Begriff 'authority-check' als String sowohl im angezeigten Coding/aktuellen Quelltext als auch global im gesamten Programm.

Beispiel FB03 - Beleg anzeigen

Liste aus TSTC:

TCODE	PGMNA	DYPNO	[...]
FB03	SAPMF05L	0100	

Der Zugriff auf die Anzeigefunktion für Buchhaltungsbelege erfolgt über das Programm SAPMF05L. Nach Aufruf von SE38, der Anzeige dieses ABAP und der Suche nach 'authority-check' global im Programm erscheint die folgende Ansicht (Auszug):

Programm	Fundstellen/Kurzbeschreibung	
... MF05LFA0	87	authority-check object 'F_BKPF_BUK' id 'ACTVT' field '02' id 'BUKRS' field bkpf-bukrs.
	99	authority-check object 'F_BKPF_BLA' id 'ACTVT' field '02' id 'BRGRU' field t003-brgru.
	209	authority-check object 'F_BKPF_BED' id 'ACTVT' field ber-act id 'BRGRU' field a01-begru.
	215	authority-check object 'F_BKPF_BED' id 'ACTVT' field '03' id 'BRGRU' field a01-begru. [...]

Hier lassen sich die Fundstellen sehr gut ablesen und die notwendigen Berechtigungsobjekte herausfiltern. Wer in die einzelnen Passagen einsteigt und den Quelltext analysiert, kann auch ergründen, welche Zustände des Programms abgefragt und wie auf diese reagiert wird, denn auf den ersten Blick ist eine solche Darstellung durchaus verwirrend. Der Quelltext sollte daher grundsätzlich eingesehen werden, da es vorkommen kann, dass einige Passagen nur in Abhängigkeit des verwendeten Transaktionscodes oder anderer Systemzustände aktiv sind. Entsprechend kann es im ersten Moment zu zum Teil widersprüchlichen Darstellungen kommen. Somit sollte jeder IV-Revisor die Grundzüge der ABAP-Programmierung erlernen. Im dargestellten Beispiel kann man bei genauer Betrachtung erkennen, dass nicht alle angezeigten Passagen für die Transaktion FB03 gelten. Vielmehr ist darauf zu achten, dass lediglich die Passagen mit der Aktivität 03 = Anzeigen zum Tragen kommen. Die übrigen Passagen gelten z.B. für den Änderungsdienst (Aktivität 02). Über die Tabellenanzeige von *TSTC* und der Eingrenzung auf Programmebene (PGMNA) mit SAPMF05L lassen sich die Transaktionen ermitteln, deren Zugänge auf die SAP-Ressourcen über dieses Programm realisiert werden.

Liste aus TSTC:

TCODE	PGMNA	DYPNO [...]
FB02	SAPMF05L	0100
FB03	SAPMF05L	0100
FB03Z	SAPMF05L	0100
FB09	SAPMF05L	0102
FB13	SAPMF05L	0102
FBD2	SAPMF05L	0100
FBD3	SAPMF05L	0100
FBM2	SAPMF05L	0100
FBM3	SAPMF05L	0100
[...]		

2.2.3 UST12 - Benutzerstamm - Berechtigungen

In dieser Tabelle können zu den einzelnen Berechtigungsobjekten die aufnehmenden Profile und die entsprechenden Feldausprägungen abgelesen werden. Dieses ist sehr hilfreich, um zum einen einen Überblick zu erhalten über die Durchdringung der Objekte in den Profilen und zum anderen über die Einzelausprägungen der Steuerungsfelder. Diese geben umfassend Hinweise auf zu prüfende Konstellationen.

Liste aus UST12:

MANDT	OBJCT	AUTH	AKTPS	FIELD	VON [...]
100	F_BKPF_BUK	F-51SA010000	A	ACTVT	01
100	F_BKPF_BUK	F-51SA010000	A	ACTVT	02
100	F_BKPF_BUK	F-51SA010000	A	ACTVT	03
100	F_BKPF_BUK	F-51SA010000	A	ACTVT	06
100	F_BKPF_BUK	F-51SA010000	A	ACTVT	07
100	F_BKPF_BUK	F-51SA010000	A	ACTVT	77
100	F_BKPF_ BUK	F-51SA010000	A	BUKRS	0100
100	F_BKPF_BUK	F-51SA026000	A	ACTVT	01
[...]					

2.2.4 AGR_1250 - Berechtigungsdaten zur Aktivitätsgruppe

Diese Tabelle zeigt die in den einzelnen Aktivitätsgruppen enthaltenen Berechtigungsobjekte mit zugehörigem Profil an. Dies ist zur Analyse der kritischen Berechtigungsobjekte des SAP-Systems sehr hilfreich.

Liste aus AGR_1250:

MANDT	AGR_NAME	COUNTER	OBJECT	AUTH [...]
100	DATENBADM..	000001	S_ADMI_FCD	DB-ADMIN..
100	DATENBADM..	000002	S_ADMI_FCD	DB-ADMIN..
100	DATENBADM..	000003	S_BTCH_ADM	DB-ADMIN..
100	DATENBADM..	000004	S_BTCH_JOB	DB-ADMIN..
100	DATENBADM..	000005	S_BTCH_NAM	DB-ADMIN..
100	DATENBADM..	000006	S_C_FUNCT	DB-ADMIN..
[...]				

2.2.5 AGR_1251 - Berechtigungsdaten zur Aktivitätsgruppe

Die Tabelle AGR_1251 geht erheblich weiter als die zuvor genannte Tabelle. Sie zeigt neben den Aktivitätsgruppen und zugehörenden Berechtigungsobjekten und Profilen die Eingrenzungen der Felder der Berechtigungsobjekte. Eine solche Übersicht hilft ganz erheblich bei der Analyse der Berechtigungsobjekte, denn hierüber lassen sich nicht nur kritische Eingrenzungen der Felder herausfiltern, sondern auch die Verursacher dieser (Aktivitätsgruppen/Profile).

Liste aus AGR_1251:

MANDT	AGR_NAME..	OBJECT	AUTH [...]	FIELD	LOW	HIGH	...
100	DATENBADM..	S_ADMI_FCD	DB-ADMIN..	S_ADMI_FCD	SM21		
100	DATENBADM..	S_ADMI_FCD	DB-ADMIN..	S_ADMI_FCD	SPTD		...
100	DATENBADM..	S_BTCH_ADM	DB-ADMIN..	BTCADMIN			
100	DATENBADM..	S_BTCH_JOB	DB-ADMIN..	JOBACTION	LIST		
100	DATENBADM..	S_BTCH_JOB	DB-ADMIN..	JOBACTION	RELE		...
100	DATENBADM..	S_BTCH_JOB	DB-ADMIN..	JOBGROUP	*		...
100	DATENBADM..	S_BTCH_NAM	DB-ADMIN..	BTCUNAME	*		
100	DATENBADM..	S_C_FUNCT	DB-ADMIN..	ACTVT	16		
100	DATENBADM..	S_C_FUNCT	DB-ADMIN..	CFUNCNAME	SYSTEM		...
[...]							

2.2.6 AGR_1252 - Orgebenen zu den Berechtigungen

Diese Tabelle zeigt zu einzelnen Aktivitätsgruppen die Felder, die durch das Customizing beeinflusst werden, und die jeweilige Einzelausprägung dieser Steuerungsfelder. Dies sind z.B. Buchungskreis, Geschäftsbereich, Werk, Kontoart usw. Die Einrichtung dieser Felder hängt vom Unternehmensaufbau und der jeweiligen Umsetzung im System ab (siehe 2.2.1).

Liste aus AGR_1252:

MANDT	AGR_NAME...	VARBL	LOW	HIGH	...
100	OE11FIAA0...	$BUKRS	0100		
100	OE11FIAA0...	$GSBER	*		
100	OE11FIAA0...	$KOART	A		
100	OE11FIAA0...	$KOART	D		
100	OE11FIAA0...	$KOART	K		
100	OE11FIAA0...	$KOART	S		
100	OE11FIAA0...	$KOKRS	*		
[...]					

Die dargestellten Tabellen geben eine umfassende Übersicht über die vorhandenen Berechtigungsverwaltungsobjekte und die jeweiligen Einzelausprägungen. Es ist naheliegend, dass der Umfang dieser Daten erhebliche Ausmaße annimmt, so dass eine Extraktbildung und Versorgung einer Datenbank zur Analyseoptimierung sinnvoll sein kann.

2.3 Berechtigungsobjekte

Das SAP-System beinhaltet mehr als 800 Berechtigungsobjekte im Standard. Sofern branchenspezifische Zusatzanwendungen eingesetzt werden, erhöht sich die Anzahl der Objekte entsprechend. Nicht alle hiervon sind für den Revisor als kritisch zu sehen, jedoch beinhalten sehr viele Objekte neben üblich-unkritischen Zugriffsausprägungen auch kritische Einzelausprägungen, so dass bei etwa 250 Objekten, die z.T. auch modulübergreifend agieren, kritische Feldwertkonstellationen vorkommen. Diese sind für den Revisor relevant.

2.4 Kritische Berechtigungsobjekte

Die kritischen Objekte sind nicht nur im Bereich der Basis zu finden, sondern auch innerhalb der Funktionsmodule wie FI, CO, MM etc. Beispiele für kritische Berechtigungsobjekte sind:

- S_RFC	- S_DEVELOP	- S_USER_AGR
- S_TABU_CLI	- S_CTS_ADMI	- S_USER_AUT
- S_TABU_DIS	- S_DATASET	- S_USER_PRO
- S_ADMI_FCD	- S_LOG_COM	- S_USER_GRP
- S_RZL_ADM	- S_TRANSPRT	- S_USER_OBJ
- F_BKPF_BUK	- F_KNA1_AEN	- F_LFA1_AEB
- F_BKPF_BED	- F_KNA1_APP	- F_LFA1_APP
- F_BKPF_BEK	- F_KNA1_BUK	- F_LFA1_BUK
- F_BKPF_BES	- F_KNA1_BED	- F_LFA1_BEK
- F_BKPF_BLA	- F_KNA1_KGD	- F_KMT_MGMT
- K_CSLA	- K_CCA	- K_CSKA
- K_CSKS	- K_VRGNG	usw.

Um Transparenz und Prüfbarkeit für die Revision zu gewährleisten, ist es sinnvoll, die kritischen Berechtigungsobjekte in Form einer Übersicht mit umfassenden kritischen Feldausprägungen und ggf. Kurzerläuterungen darzustellen. Eine solche Übersicht kann nicht nur die laufende Arbeit erleichtern, sie erhöht insbesondere die Effektivität bei Wiederholungsprüfungen.

3 Ausgesuchte Berechtigungsobjekte

Entsprechend kann eine solche Darstellung z.B. wie folgt aussehen:

Berecht.obj.		**Feld 1** *Prüftabelle*	**Feld 2** *Prüftabelle*	**Feld 3 ....** *Prüftabelle*	**Bemerkung**
	Kritische Berechtigung	Krit. Feldwert	Krit. Feldwert	Krit. Feldwert	
F_BKPF_BUK Buchhaltungs-belege Berechtigung auf Buchungs-kreise		**ACTVT** *TACT/TACTZ*	**BUKRS** *T001*		Die nachfolgenden BO's dienen zur Steuerung der Zugriffe auf Buchhaltungs-belege (BKPF/BSEG).
	Hinzufügen / Ändern	01/02			
	Sperren/Lösch.	05/06			
	Aktivieren/ Generieren	07			
	Erfassen / Vor-erfassen	76/77			
	Generalberecht.	*	*		
F_BKPF_BED Einschränkung der Erfassung und Bearbeit. von Belegposit. auf Debitoren-konten		**ACTVT** *TACT/TACTZ*	**BRGRU** *TBRG*		ACTVT 01 gilt bei den BO's des Moduls FI z.T. auch als Buchungsberechtigung. ACTVT 10 hat hier keine Bedeutung.
	Hinzufügen	01			
	Ändern	02			
	Generalberecht.	*****	* / FC*		
F_BKPF_BEK Kontenberechti-gung Kreditor		**ACTVT** *TACT/TACTZ*	**BRGRU** *TBRG*		
	Hinzufügen	01			
	Ändern	02			
	Generalberecht.	*****	* / FC*		

[...]

Die Entwicklung einer solchen Tabelle ist sehr arbeitsintensiv. Leider sind umfassende Übersichten mit Erläuterungen zu Einzelausprägungen und den jeweiligen Referenzprüftabellen der Felder kaum vorhanden. Zusätzlich ist die SAP-Dokumentation über "Werkzeuge - Administration - Benutzer-pflege - Berechtigung (SU03) - Info - Objektliste m. Doku" leider zumeist unzureichend, zumindest aber sehr umständlich. Weiterhin sind in solchen Tabellen die unternehmensspezifischen Besonder-heiten zu berücksichtigen, so dass es sich lohnt, selbst solche Tabellen für die einzelnen Module zu entwickeln.

4. Fazit

Die Beurteilung, welche Objekte in welcher Ausprägung kritisch sind, muss jedes Unter-nehmen und somit auch jeder IV-Revisor für sich selbst treffen. Die Entwicklung und Bereitstellung vorgenannter Tabellen kann eine sinnvolle Hilfestellung sein bei der Bewältigung der eigenen Bemühungen, kritische Objekte inklusive ihrer Einzelausprägungen zu identifizieren und zu dokumen-tieren.

Ausgesuchte Literatur:

Christoph Wildensee	Ausgesuchte Berechtigungsobjekte des SAP R/3 - Systems als Prüfungsansatz für die IV-Revision - Eine Übersicht - Teil 1 bis 3 für Basis, FI & CO ReVision III/2001ff, Ottokar-Schreiber-Verlag, Hamburg http://www.osv-hamburg.de	
Jan van Acken	AIS Das Audit-Information-System von SAP Ein Werkzeug für die Revision ? ReVision I/2000, Ottokar-Schreiber-Verlag, Hamburg	
Thomas Tiede	SAP R/3 Ordnungsmäßigkeit und Prüfung des SAP-Systems (OPSAP) Ottokar-Schreiber-Verlag, Hamburg http://www.ibs-hamburg.com	2000
s.a. Roger Odenthal	Vorgehensmodell zur Prüfung des Berechtigungswesens in einer SAP R/3 – Umgebung Zeitschrift Interne Revision (ZIR) 3/2000	

www.wildensee.de/veroeff.htm

Zeitschrift Interne Revision (ZIR) 2002