

Sicherheitskonzeption in SAP R/3® – Regelungsbedarf über die Berechtigungsdefinition und -vergabe hinaus

Von Dipl.-Betriebswirt Christoph Wildensee, Hannover ¹

Einführung

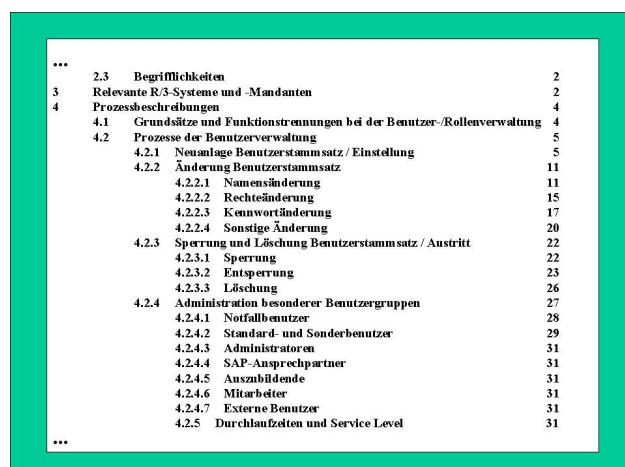
In vielen Unternehmen läuft SAP R/3 reibungslos – gefahren von erfahrenen Administratoren und Systemtechnikern. Änderungen im Customizing werden jedoch auf Zuruf durchgeführt, wenn es die Notwendigkeit durch Fachbereichs- oder Systemerfordernisse gebietet. Ein dokumentiertes Berechtigungskonzept beinhaltet dort meist lediglich Regelungen, die die **Vergabe und Verwaltung** von Berechtigungen betreffen. Dies ist jedoch beim Betrieb eines solch umfassenden DV-Konstruktes nicht ausreichend, um Revisionsstandards zu erfüllen. Notwendig ist eine Zusammenführung von Regelungen, die den gesamten „Life-Cycle“ des SAP-Systems und aller Komponenten dokumentiert, um den Betrieb nachvollziehbar, nachhaltig und mit Soll-Vorgaben zu gewährleisten.

Der SAP R/3 - Rahmen

Ein **Rahmenleitfaden** muss als Basis des Berechtigungskonzeptes gesehen werden, der alle zu regelnden Punkte systematisch aufnimmt und verbindliche Regelungen beinhaltet. Dabei soll er nicht nur für die technische Seite (Administration, Customizing) als Dokumentation und Nachschlagewerk dienen, sondern auch für die Key-User der involvierten Fachbereiche - den Modulnutzern - im Tagesgeschäft und letztlich auch für die nachvollziehenden Gremien (Datenschutz, Revision, Betriebsrat, IT-Sicherheitsbeauftragter etc.) als Dokumentation der Soll-Vorgaben, um sie am Ist spiegeln zu können. Es ist z.B. oft feststellbar, dass die DV-Koordinatoren der Fachbereiche zu wenig Ein- und somit Übersicht über das System an sich haben, so dass die Beantragung und der Nachvollzug z.B. über Rechte, aber auch über Einstellungen in den Modulen erschwert wird. Ein zentral bereitgestelltes Instrument wie der SAP R/3 – Rahmenleitfaden soll somit alle Informationsbedarfe der Recherchierenden abdecken. Funktionsbeschreibungen der Module soll er dabei selbstverständlich nicht beinhalten.

Inhalte eines Rahmenleitfadens

Der administrative Aufwand in SAP R/3 ist sehr umfangreich, er reicht vom Einstellen des Systems selbst und der angrenzenden Komponenten wie Betriebssystem, Datenbank etc., dem Verwalten von Updates/Patches, dem Anpassen der Funktionalitäten über Eigenentwicklung bis zum Erteilen von Rechten auf und dem Verwalten von bestimmte Funktionen und Ressourcen. Der Regelungsbedarf ist mannigfaltig. Entsprechend umfangreich ist auch der Leitfaden, der zielführend gegliedert sein muss.



...	2.3	Begrifflichkeiten	2
3		Relevante R/3-Systeme und -Mandanten	2
4		Prozessbeschreibungen	4
	4.1	Grundsätze und Funktionstränkungen bei der Benutzer-/Rollenverwaltung	4
	4.2	Prozesse der Benutzerverwaltung	5
	4.2.1	Neuanlage Benutzerstammsatz / Einstellung	5
	4.2.2	Änderung Benutzerstammsatz	11
	4.2.2.1	Namensänderung	11
	4.2.2.2	Rechteänderung	15
	4.2.2.3	Kenwortänderung	17
	4.2.2.4	Sonstige Änderung	20
	4.2.3	Sperrung und Löschung Benutzerstammsatz / Austritt	22
	4.2.3.1	Sperrung	22
	4.2.3.2	Entsperrung	23
	4.2.3.3	Löschung	26
	4.2.4	Administration besonderer Benutzergruppen	27
	4.2.4.1	Notfallbenutzer	28
	4.2.4.2	Standard- und Sonderbenutzer	29
	4.2.4.3	Administratoren	31
	4.2.4.4	SAP-Ansprechpartner	31
	4.2.4.5	Auszubildende	31
	4.2.4.6	Mitarbeiter	31
	4.2.4.7	Externe Benutzer	31
	4.2.5	Durchlaufzeiten und Service Level	31
...			

Abb. 1: Beispiel Teilinhaltsverzeichnis Leitfaden

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

Nachfolgend soll in tabellarischer Form beispielhaft dargestellt werden, welche Themen in einem Rahmenleitfaden eingearbeitet werden sollten (kein Anspruch auf Vollständigkeit).

Customizing, Administration, Dokumentation

- ➔ Unterscheidung Produktions- / Test- [Integrations-] / Qualitätssicherungssystem
- ➔ Schulungssystem: Datenbestand und Anonymisierung / Pseudonymisierung, zu beachten: Kostenstellen (personalführende KSt, KSt von Einzelpersonen), Kostenarten, Reporting etc.
- ➔ Unterscheidung der Administratoren und Sonderuser (Modul-Administratoren, CPIC, SAP*, DDIC, HotlineSAP / Earlywatch etc. je System: ggf. SAP-Auslieferungsstatus, Kennwörter, Sperrung, Protokollierung usw.
- ➔ Systemstatus: Systeme, Instanzen, Prozesse, Verbuchung, User- / Transaktions- / System-sperrungen, Änderbarkeitsstatus und –steuerung etc.
- ➔ Notfalluser-Konzept: User NOTFALL, Kennworthinterlegung, zweigeteiltes Kennwort, Nutzungserlaubnis, Kennwortdoppelerstellung und –verschluss
- ➔ Initialkennwortvergabe: Erstellung, Weitergabe zum User, Sperrung nach welcher Zeit bei Nicht-Nutzung
- ➔ Kennwortkonventionen, unzulässige Kennwörter etc.
- ➔ Systemparameter: Customizing jedes Systems, Dokumentation und Replik / Sicherung, Einstellungen zur R/3-Oberfläche der Benutzer, zur Steuerung der Berechtigungsprüfungen, zur Benutzeridentifizierung und –authentifizierung und zum Logging, Dokumentation von Soll-Vorgaben und Ist-Werten, regelmäßiger Delta-Check, Meldewesen bei Systemänderungen
- ➔ Single-Sign-On (SSO): Parametrisierung, Synchronisation etc.
- ➔ Definition von Aufgaben / Kompetenzen / Verantwortung / Vorgehen im Customizing, bei Systemkopien u.ä. (z.B. auch Ablauforganisation, Terminierungen etc.)
- ➔ AIS: Customizing und Dokumentation, Aufbau von aufgabenorientierten bzw. fachbereichs-spezifischen, vorparametrisierten Berichtszweigen, Laufzeitbeschränkungsdefinitionen etc.
- ➔ Organisation / Business-Strukturen: Dokumentation der Einstellungen: BUKRS, KOKRS, Perioden, Belegarten, Nummernkreise, Klassifizierungen von Mitarbeitern, Tabellen, ABAP's etc., Infotypen, Subtypen, Mitarbeitergruppen etc., Namenskonventionen, Namensräume etc.
- ➔ SAP-Prozesse und Freigaben
- ➔ Schnittstellen zu anderen R/3-Systemen und zur weiteren DV-Landschaft, RFC, iDoc etc., Dokumentation und Freigabeverfahren, Funktionsbausteinaufrufe, Unterscheidung kritischer Aufruf- / Ansteuerungsmöglichkeiten, Schnittstellenbeschreibungen
- ➔ eProcurement: Schnittstellendefinition zwischen externem Tool (z.B. Enterprise Buyer Prof. [EBP]) und SAP R/3, Verfahrensbeschreibung der Datenübergabe und des Berechtigungs-konzeptes, Zugriff für Fachbereiche

- ➔ Batch-Input: Steuerung der Zugriffe (wer darf Batch-Input nutzen, für welche Systeme, Zwecke, Fachbereiche wird es freigegeben etc.), Namenskonventionen, Berechtigungsobjekteingrenzung, Klassifizierung, Verfahrensbeschreibung, Fachbereichsspezifika
- ➔ Tabellenpflege: Steuerung der Zugriffe, restriktiver Einsatz, Berechtigungsobjekteingrenzung, Nutzung der Klassifizierung etc.
- ➔ Debugging: Wer darf im Debugging arbeiten, restriktiver Einsatz des Edit-Modus, Vier-Augen-Prinzip durch unzureichende Protokollierung, nur Einsatz durch Fachbereichserfordernis, Dokumentation revisionssicher (vorher/nachher), zentrale Dokumentation zwecks Nachvollzug und Abgleichmöglichkeit mit SM21 => Meldungskennungen A14/A19
- ➔ Spool-Verwaltung: Berechtigungsobjekteingrenzung, kritische Ausprägungen, Klassifizierung
- ➔ Job-Verwaltung: Berechtigungsobjekteingrenzung, kritische Ausprägungen, Klassifizierung, sofern externes Jobsteuerungs- u/o ggf. Druckoutputmanagementsystem zum Einsatz kommt: Definition von Sicherheitsmaßnahmen, auch im Hinblick auf Schnittstellen zum Betriebssystem (Job-Weitergabe, Druck-Server, Vertrauensbeziehungen, auch Archivierung etc.)
- ➔ Computing Center Management System (CCMS): Monitoring, Leitstand, Datenbanktools, restriktiver Einsatz
- ➔ Employee Self Service (ESS) / anwendungsübergreifendes Arbeitszeitblatt (cross application time sheet (CATS))
- ➔ HR: Organisations- und Steuerungsstrukturen der Personalwirtschaft, z.B. Organisation: Personal(teil)bereich, Mitarbeitergruppe / -kreis, Personalabrechnungskreis, Infotypen / Subtypen, Lohnarten etc.; Steuerung: P_ORGIN, P_ORGXX, P_PERNR, P_PCLX, P_PY*, P_ABAP etc.
- ➔ Human Information System (HIS) – vorparametrisierte Auswertungen für HR
- ➔ Reporting / Berichtsbäume / Infosysteme der Einzelmodule, Query-Tools (auch externe)
- ➔ Änderungshistorie, Protokollierung und die Auswertung dieser Informationen: SysLog, AuditLog, Unterscheidung kritischer Meldekennungen, protokollierte User je System etc.
- ➔ Festlegung von systemkritischen (zu überwachenden) Zuständen, kritische / sensible Daten / Informationen und kritische Berechtigungsobjektausprägungen / -konstellationen (Tabellen, Reports, Transaktionen, Berechtigungsobjekte, Objekteingrenzungen) [...]

Betriebssystem, Datenbank

- ➔ Übersicht Betriebssystem- und Datenbankdienste, Ablagestrukturen
- ➔ kritische Dienste und Verzeichnisse auf den Application-Servern und den Freigaben hierauf
- ➔ Dokumentation der Betriebssystem- und Datenbankadministratoren
- ➔ zu überwachende Dienste, Verzeichnisse, Dateien; Vertrauensbeziehungen und deren Wirkung
- ➔ Remote-Zugriffe und Internet-User etc.
- ➔ Definition von Sicherheitsmaßnahmen auf Betriebssystem- und Datenbankebene, Einbezug der SAP R/3-Sicherheitsleitfäden, auch Datenschutzerfordernungen integrieren [...]

Changemanagement

- ➔ Systemänderungen durch Umgang mit Hot Packages, Legal Change Packages und Eigenentwicklungen incl. Übernahme in die Produktionsumgebungen, Unterscheidung von Fehlerkorrekturen / Erweiterungen durch Extern-Anstoß und Fehlerkorrekturen / Neue Funktionen durch Intern-Anstoß
 - > kundeneigener Entwicklungs- / Namensraum
 - > Zeitplanung / Terminierungen
 - > Ressourcenplanung
 - > Dokumentation
- ➔ Definition von Standards bei der Implementierung neuer Funktionen
- ➔ Testverfahren: Definition, Durchführung, Verantwortung, Abnahme, Dokumentation
- ➔ Test systemgestützt erleichtern, Automation von Testfällen, sofern möglich
- ➔ regelmäßige Verifizierung von Testverfahren, Katalog abgestimmter Testverfahren, ggf. prozessbezogen
- ➔ Notfallplan für Systemstillstand
- ➔ Entwicklung: Regelung je System, Trennung von Entwicklung und Produktionsumgebung, Transportwesen / -auftrag, Entwickler- und Objektschlüssel
- ➔ Report-Entwicklung: QS-Maßnahmen
 - > Systemabgrenzung: Welche Systeme werden für welche Aufgaben genutzt ?
 - > Dokumentation / Entwicklerrichtlinie, Namenskonventionen, standardisierte Doku-Pflicht
 - > Abnahmetest der Funktion, Handhabung, Ergebnisse, Zielkonformitätsuntersuchung
 - > Transportwesen
 - > Abgrenzung der Einbindung von Revision / bDSB / IT-Sicherheit in Abhängigkeit des Manipulationsgrades auf Tabellen
- ➔ Computer Aided Test Tool (CATT)
 - > Ziel: Frühzeitiges Aufzeigen von Fehlerquellen, Vereinheitlichung / Standardisierung und beliebige Wiederholbarkeit von Testabläufen, Automatisierung von Testabläufen, Erzeugung von Schulungsdaten, einheitliche Dokumentation von Tests
 - > beinhaltet: Aufzeichnungstool für Prozesse, Workbench zur Verwaltung von Testprozeduren, Wiedergabebereich für Testprozesse
 - > benötigt: Geschäftsprozessdefinition, beteiligte Transaktionen und zugrundeliegende Daten
 - > Grundsatz: Nicht alle Prozesse und Transaktionen können aufgezeichnet werden => Abgrenzung manuell vs. automatisiert; zu beachten: Öffnung/Änderbarkeit des Systems
 - > Beantragungs- und Freigabedefinition, CATT-Testkatalog [...]

Berechtigungsvergabe und –verwaltung

- ➔ Grundsätze der Berechtigungsvergabe und –verwaltung, Funktionstrennungsprinzip, Restriktivhandhabung, Prozessübersicht der B.-vergabe und –verwaltung, Namenskonventionen für die Elemente der B.-verwaltung, Definition von Aufgaben, Kompetenzen, Verantwortung

- ➔ Benutzerstammsatz
 - > Neuanlage: Welche Daten werden gepflegt ? Klassifizierung von Nutzern, wer darf Neuanlage durchführen, welche Rechte sind mit der Steuerung verbunden ? Wie sind diese aufzuteilen auf die Administratoren ?
 - > Änderung: Stammdatenänderung, Rechtezuweisungsänderung, Kennwortänderung
 - > Sperren / Löschen: Wer darf eine Sperrung / Entsperrung / Löschung veranlassen und durchführen ? Sonderfall Externe, Befristung, Austritt eines Nutzers aus dem Unternehmen
- ➔ Rollendefinitionen
 - > Anlegen / Ändern / Löschen von Rollen
 - > Fachbereichstest der Rollen, Abnahme- / Freigabeverfahren, Überführen in Produktionsumgebung, Namenskonventionen, Dokumentation der Rollen
 - > Kontrollverfahren bei der Rollendefinition (z.B. bei Rollenkollisionen)
 - > Einstellungen zum Transport von Rollen und Benutzerabgleich
 - > Einbezug von Revision / bDSB / IT-Sicherheit von kritischen Rollen
- ➔ Profilgenerator (PFCG)
 - > Wer nutzt den Profilgenerator bei welchen Aufgaben ?
 - > Profilgenerator ist auch als Nachvollzugsinstrumentarium einsetzbar
 - > Ausschließlichkeitsprinzip zur Nutzung von PFCG bei der Rollendefinition vs. Grundsatz der PFCG-Nutzung bei der Rollendefinition mit gelegentlicher manueller Rollendefinition im Bedarfsfall (Sonderuser)
 - > Überprüfung der Profilgenerator-Ergebnisse durch wen, wie, Dokumentation und Veränderungsprozedur
 - > Grundsatz der Redundanzfreiheit von Berechtigungen in den Rollendefinitionen, Sicherstellung und Nachvollzug
- ➔ Profile und Berechtigungen
 - > Namenskonventionen und Dokumentation der Elemente
 - > Kritische Berechtigungen / Berechtigungsobjektkonstellationen und -kombinationen
 - > Definition und Dokumentation überwachungsbedürftiger Berechtigungsobjektausprägungen und Transaktionen, bei denen eine restriktive Handhabung notwendig ist
 - > Zustimmungsverfahren bei Zugriff auf überwachungsbedürftige Berechtigungen
 - > Übersicht / Dokumentation über Profile / Berechtigungen zu definierten Rollen
 - > Definition nachgelagerter, regelmäßiger Kontrollen der Rollen / Berechtigungen / Profile
- ➔ Sonderuser und deren Behandlung
 - > Systemuser, Notfall, Administratoren, Key-User der Fachbereiche (DV-Koordinatoren, SAP-Modul-Ansprechpartner o.ä.)
 - > Auszubildende (ggf. als Sammler umfassender Berechtigungen durch das ‚Durchlaufen‘ in den einzelnen Unternehmensbereichen und dem häufigen Einbeziehen in das Tagesgeschäft, zu beachten: zeitlich befristete Vergaben von Rollen möglich !)
 - > Externe (Berater, Wirtschaftsprüfung, Betriebsprüfung)
 - > Sicht-User (Revision, bDSB, IT-Sicherheit, ggf. Betriebsrat), zu regeln: umfassende Sicht, CCMS-Funktionalitäten, Tabellen, ABAP-Workbench etc. [...]

Berechtigungen Fachbereiche

- ➔ Übersicht der Menü- und Modul-Rollen im Unternehmen je Fachbereich
- ➔ Zur-Verfügung-Stellen eines Nachvollzugsinstrumentariums für die Fachbereiche, z.B. AIS
- ➔ Definition einer zentralen Anlaufstelle zur Klärung von Fragen zum Berechtigungskonzept, z.B. Revision und bDSB, zusätzliche Funktionalitätsbereitstellung für diese, z.B. CheckAud SAP R/3

Sonstiges

- ➔ Aufbewahrungspflichten und zu beachtende Fristen
- ➔ Archivierungssysteme (Schnittstellen, Sicherungs- und QS-Maßnahmen)
- ➔ gesetzliche Anforderungen
- ➔ Formularwesen
- ➔ Ansprechpartner und Verantwortliche im Unternehmen
- ➔ Schulungskonzept
- ➔ Interne Hotline: Aufgaben, Kompetenzen, Verantwortung, Definition einer Ablauforganisation
- ➔ Qualifikationsdefinitionen für Key-User [...]

Fazit

Meines Erachtens reicht allein die Festlegung von Rahmenbedingungen für die Berechtigungssteuerung längst nicht aus, um ein solch umfassendes System nachvollziehbar zu fahren. Die unterschiedlichen SAP-Nutzergruppen und deren jeweiliger Informationsbedarf sind so zu berücksichtigen, dass bei einer Zusammenführung von verbindlichen Regelungen zu einem umfassenden SAP R/3-Rahmenleitfaden ein sinnvolles Betriebsführungs- und Nachvollzugsinstrumentarium zur Verfügung gestellt werden kann. Lediglich systemkritische / sensible Informationen wie IP-Adressen u.ä., die einen Geheimhaltungsstatus genießen **müssen**, sollten aus dem zentralen Leitfaden herausgelöst werden bzw. bleiben.

Literatur:

- | | |
|-----------------------------|---|
| Thomas Tiede | Ordnungsmäßigkeit und Prüfung des SAP-Systems, OSV |
| Geesmann, Glauch, Hohnhorst | SAP R/3 Datenschutz und Sicherheitsmanagement, OSV |
| Christoph Wildensee | Ausgesuchte Berechtigungsobjekte des SAP R/3-Systems als Prüfansatz für die IV-Revision, ReVision III/2001-I/2002 |
| Christoph Wildensee | SAP R/3 – Besonderheiten des Systems bei der Prüfung des Berechtigungskonzeptes, ZIR 4/2002 |
| Christoph Wildensee | www.wildensee.de/veroeff.htm |

Revisionsspezifische Ordnungsmäßigkeitskriterien:
u.a. GoB, HGB, AktG, ergänzend KonTraG, FAMA/ERS FAIT1, IDW PS330