

Merkblatt für die Vorbereitung von SAP-HANA Prüfungen

1. Merkblatt und Prüfungsziel

Das vorliegende Merkblatt möchte zu einer friktionsfreien Prüfung beitragen und die Einrichtung einer hierfür erforderlichen Nutzerkennung unterstützen. Sollen einzelne Anforderungen in seltenen Fällen nicht erfüllt werden können, bitten wir um rechtzeitige Kontaktaufnahme und Erörterung. Wir überlegen gemeinsam mit zuständigen SAP-Verantwortlichen Alternativen oder entscheiden, ob eine beauftragte Prüfung unter eingrenzenden Randbedingungen durchgeführt werden kann.

Unsere Prüfungen werden durch erfahrene Mitarbeiter durchgeführt. Hierbei werden sowohl Ordnungsmäßigkeitsaspekte des SAP-Einsatzes (auf Applikations- und Datenbankebene) gesichtet, als auch Techniken der computergestützten Datenprüfung in einer SAP-HANA-Umgebung angewendet. Die beschriebenen Prüfungsinhalte werden direkt innerhalb der SAP-Applikation und der HANA-Datenbank erarbeitet.

2. SAP-Arbeitsplatz des Prüfers

Der Prüfer benötigt einen *eigenen Zugang zur SAP-Applikation (z.B. S4/HANA) und zur HANA-Datenbank*. Günstig wäre es, wenn über einen Personalcomputer auf die aufgeführte Prüfungsumgebung SAP-System zugegriffen werden könnte. Auf dem lokalen PC bzw. innerhalb des Netzwerkes muss der Prüfer *über ein Verzeichnis mit vollen Lese- und Schreibrechten verfügen, auf welches im Bedarfsfall Daten aus dem SAP-System abgelegt werden können*.

3. Notwendiger Berechtigungsumfang auf Applikationsebene

3.1. Bei Berechtigungszuordnung aus Berechtigungsrollen (Profilgenerator)

SAP beinhaltet *standardmäßig* Rollentemplates (Rollenvorlagen) für die Aufgaben der in- und externen Revision. Diese sind von SAP speziell für die Revisionsarbeit (nur Ansehberechtigungen) vorbereitet und können mit überschaubarem Aufwand (Ergänzung von Organisationsebenen) an betriebliche Erfordernisse angepasst werden. Hierzu sind nachfolgende Schritte erforderlich:

- Rollen identifizieren und in den Kundennamensraum überführen
Vorbereitete Berechtigungsrollen enthalten als Einzel- und Sammelrollen die Bezeichnung „*AUDIT*“ und können so ermittelt werden.
- Rollensystematik

Es gibt je *zwei Versionen* von Prüfer-Berechtigungsrollen entsprechend dem nachfolgenden Beispiel

- SAP_AUDITOR_BA_CFM (**Menü** Kaufmännisches Audit, Treasury)

Diese Rollen ohne abschließendes „_A“ beinhalten *keine Berechtigungen!* Der Prüfer erhält hierüber lediglich die für seine Tätigkeit erforderliche und angepasste SAP-Menüoberfläche (Benutzermenü) mit der Bezeichnung (AIS - Audit Information System).

3.2. Bei Berechtigungszuordnung aus SAP Standard-Berechtigungsprofilen

Soweit in seltenen Fällen schnell und ohne Aufwand Revisionsberechtigungen zugeordnet werden müssen, kann alternativ auf die ältere Form der Berechtigungszuordnung mittels SAP-Standardberechtigungsprofilen zurückgegriffen werden.

Für ihre speziellen Prüfungsanforderungen benötigt die Revision hier einen möglichst umfassenden Berechtigungsumfang - allerdings begrenzt auf Anzeigeaktivitäten. Geeignete Profile sind an den Endungen „ANZ“ oder „SHOW“ erkennbar. Dies gilt für alle Module, z.B. F_ANZ, M_ANZ, etc., deren Profile ausnahmslos zugeordnet werden müssen. Hinzu kommen unabdingbare Anzeigetransaktionen für die SAP-Basiskomponente die mit dem Profil „S_A.SHOW“ zur Verfügung gestellt wird.

3.3. Ergänzende Berechtigungen

Den speziellen Aufgaben der Revision entsprechend ist es sinnvoll, über die aufgeführten Berechtigungsrollen hinaus nachfolgende Sachverhalte zu prüfen und sicher zu stellen:

- Berechtigung für Sichtungen auf HANA-Datenbankebene
Unabhängig von weiteren prüfenden Zugriffsoptionen auf die HANA-Datenbank sollte die Transaktion "DBACOCKPIT" ermöglicht werden. Hierzu bedarf es zusätzlich folgender Berechtigungen für die Revisionskennung:
 - Objekt S_TCODE
Eintrag "DBACOCKPIT" für das Feld TCD.
 - Objekt S_ADMI_FCD
u.a den Eintrag "ST0R" (Berechtigung zum Auswerten von Traces)
 - Objekt S_DBCON
Eintrag "03" (Ansehen) und "71" (Analysen) für das Feld ACTVT sowie Einträge für den Servernamen der HANA-Datenbank, den Datenbanknamen und den Datenbankbenutzer
 - Objekt S_TABU_SQL
Eintrag "33" (Lesen) für das Feld Aktivität sowie den logischen Datenbanknamen, die Tabellennamen (z.B. "**") und den Tabelleneigentümer auf Datenbankebene (z.B. System oder "**").
- Weitere Transaktionsberechtigungen (Objekt S_TCODE)
Informationen zu spezifischen SAP-Sachverhalten, Tabellen, LOG-Einträgen, Parametern, Änderungsbelegen, Customizing und ähnliche, verlangen den Zugriff über vielfältigste Transaktionen insbesondere auch aus dem SAP-Basisbereich. Da *kritische (ändernde) Aktionen bereits über den Aktivitätslevel der SAP-Prüferrollen ausgeschlossen werden* und im Einzelfall nicht bestimmt werden kann, welche Transaktionen zur Ermittlung bestimmter Informationen herangezogen werden, ist eine darüberhinausgehende Einschränkung prüferischer Aktivitäten auf Transaktionsebene *wenig sinnvoll*. Wünschenswert wäre u.a. der Eintrag „S*“ für das Berechtigungsobjekt S_TCODE).

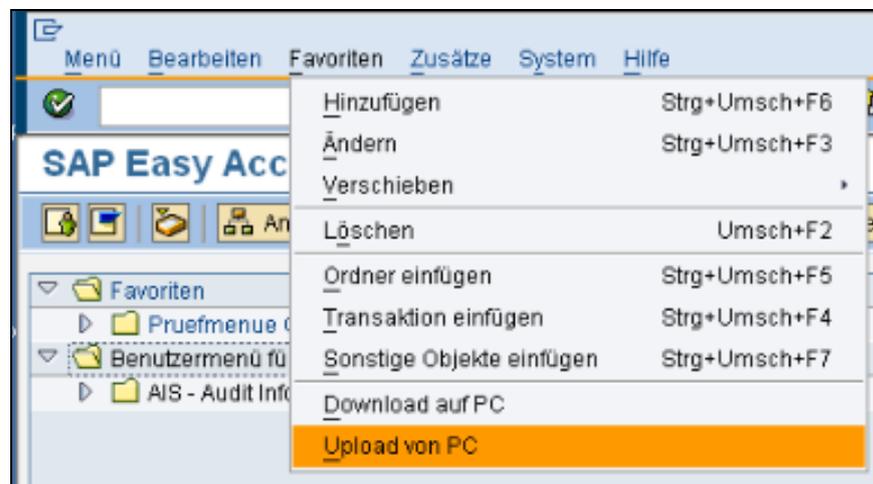
- 4 -

- Download-Berechtigung für Reports und Tabellen (Objekt S_GUI)

Der Einsatz spezieller Revisionsprogramme zur Analyse von SAP-Daten auf lokalen betrieblichen Rechnern erfordert eine Downloadberechtigung (Feld Aktivität mit den Einträgen "60", "61" und "02" oder "**") für den Prüfer.

- Down- und Upload-Berechtigungen für Favoriten

Für spezielle Prüffelder stehen vorbereitete Prüferoberflächen auf der Grundlage von Menü-Favoriten zur Verfügung, welche zwischen den Prüfungsberechtigten ausgetauscht und dem jeweiligen SAP-Revisionsnutzer im Bedarfsfall zugeordnet werden müssen. Hierzu wird die Down- und Upload-Berechtigung benötigt.



- Pflege eigener Benutzervorgaben (Festwerte und Parameter mittels SU3)

Für die Zuordnung und Konfektionierung von Druckern sowie Einstellungen zu Downloadpfaden bzw. sonstigen Organisationselementen oder Selektionskriterien müssen eigene Benutzervorgaben (Festwerte und Parameter) für den Prüfer zu pflegen sein.

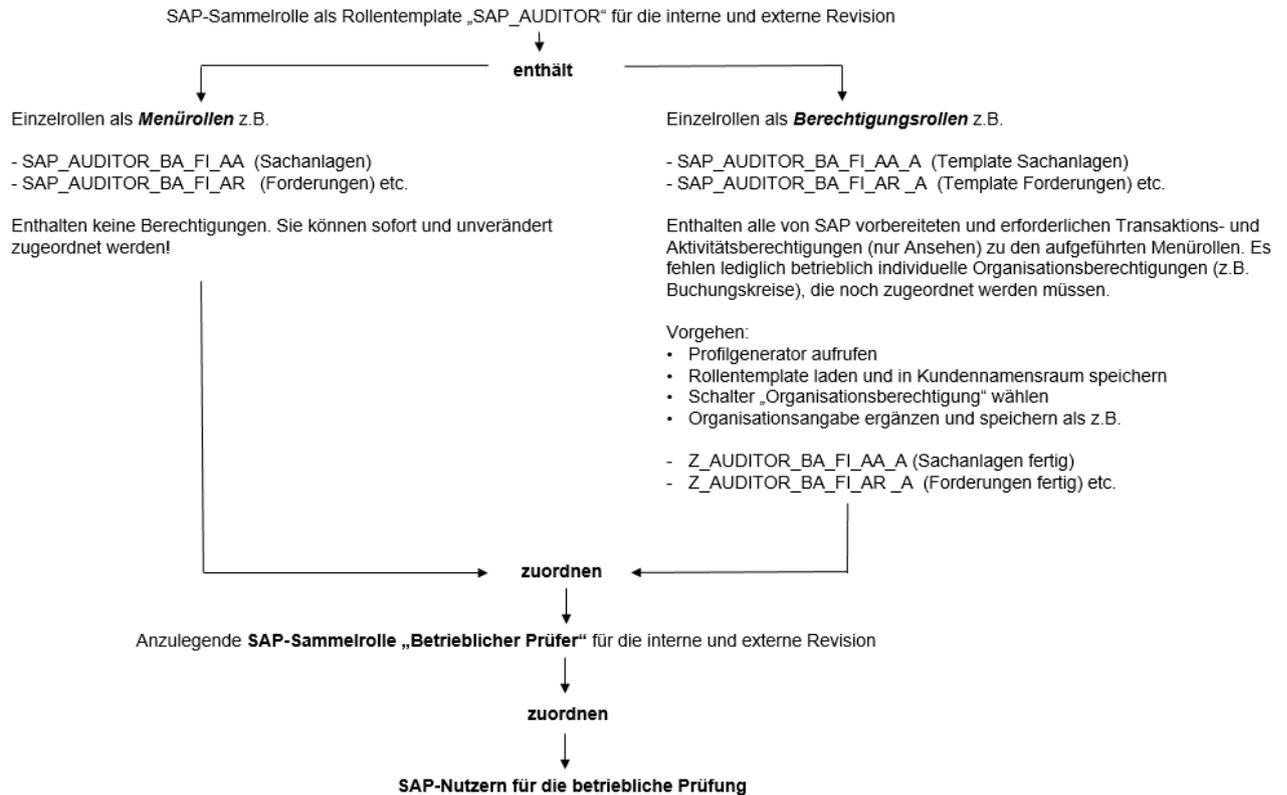
- Nutzung von Variantentechnik, Hintergrundverarbeitung und Job-steuerung

Komplexe Revisionsfragen und damit verbundenen SAP-Auswertungen sollen mittels Varianten zur wiederholten Verwendung innerhalb des SAP-Systems durch die Revision gespeichert und im Hintergrund (zu lastschwachen Zeiten oder kontinuierlich z.B. als jährlichen Analyse) eingeplant und freigegeben werden können.

- Änderungsberechtigung zu Tabellen „TVARV / TVARVC“

Zur Gestaltung dynamischer Report-Varianten müssen Prüfer, abseits der sonstigen Begrenzung auf Ansehberechtigungen, innerhalb dieser speziellen Tabellen Variable eintragen und Werte zuordnen können. Die Eingrenzung der Änderungsberechtigung auf diese einzelnen Tabellen unterstützt SAP mit dem neuen Berechtigungsobjekt „S_TABU_NAM“, welches aktiviert werden sollte. Einzelheiten finden sich in OSS-Hinweis 1481950.

4. Zusammenfassende Darstellung des Vorgehens



5. Zuordnung der Benutzerkennungen zu Query-Benutzergruppen

SAP stellt der Revision standardmäßig einige fertige Prüfprogramme (Queries) zur Verfügung. Damit diese nutzbar sind, müssen die Revisionskennungen in folgende Query- Benutzergruppen:

/SAPQUERY/AU	Audit
/SAPQUERY/AM	Anlagenmanager

eingetragen werden. Dieses gilt auch dann, wenn der SAP Revisionsnutzer nicht mit der Berechtigung zum Anlegen oder Ändern von Queries oder Quick-Views ausgestattet ist.

6. Notwendiger Berechtigungsumfang auf HANA Datenbankebene

6.1. Einrichtung für alternative Zugriffsoptionen zur HANA-DB

Wenn für die HANA-Datenbankadministration unabhängig von der Applikationsebene das HANA-Studio (ECLIPSE einschließlich zugehöriger HANA ADMIN APPS) oder das HANA-Cockpit eingesetzt werden, sollte die Revision für ihre Prüfungen ebenfalls einen (lesenden) Zugang zu diesen Werkzeugen erhalten. Dieses beinhaltet u.a die ergänzende Einrichtung eines personalisierten HANA-Datenbanknutzers und dessen Ausstattung mit einer HANA-DB-Prüferrolle.

6.2. Konfektionierung der HANA-DB Prüferrolle

Bei der Einrichtung einer Prüferrolle zur HANA-Datenbank sollten die nachfolgenden Berechtigungen berücksichtigt werden:

- Rechte (Privileges) der Rolle "PUBLIC"
Die Rolle "PUBLIC" bildet mit ihren lesenden Rechten den Grundstock der Prüferrolle.
- Erweiterungen zur Rolle "PUBLIC" für prüfende Zwecke
Entsprechend der Aufgaben der Internen Revision sollte die **Rolle "PUBLIC"** mit zusätzlichen Zugriffsberechtigungen Tabellen und Views ergänzt werden. Hierzu findet sich nachfolgend ein Vorschlag, der ggf. vor dem Hintergrund konkreter Prüfungssituationen erweitert werden muss:

```
role IR::HANA_AUDITOR {

// Prüferrolle

// Package Privilege zur Anzeige des gesamten Repositories
package '.REPO_PACKAGE_ROOT':
    REPO.READ;

// System Privilege zur Anzeige aller Schemata
system privilege:
    CATALOG READ;

// Application Privileges
... // Erforderliche XS-Berechtigungen

// Object Privileges
catalog schema 'SAP<sid>': SELECT; //Zugriff auf die Daten des ABAP Stack
catalog sql object 'SYS'.REPOSITORY_REST': EXECUTE;
catalog sql object '_SYS_XS'.HTTP_DESTINATIONS': SELECT;
catalog sql object '_SYS_XS'.OAUTH_APP_CONFIG': SELECT;
catalog sql object '_SYS_XS'.OAUTH_APP_CONFIG_SCOPES': SELECT;
catalog sql object '_SYS_XS'.OAUTH_CLIENT_CONFIG': SELECT;
catalog sql object '_SYS_XS'.RUNTIME_CONFIGURATION': SELECT;
catalog sql object '_SYS_XS'.SAML_PROVIDER_CONFIG': SELECT;
catalog sql object '_SYS_XS'.SQL_CONNECTIONS': SELECT;
catalog sql object '_SYS_REPO'.OBJECT_HISTORY': SELECT;
catalog sql object '_SYS_REPO'.PRODUCTS': SELECT;
catalog sql object '_SYS_REPO'.PRODUCT_INSTANCES': SELECT;
catalog sql object '_SYS_REPO'.DELIVERY_UNITS': SELECT;
catalog sql object '_SYS_REPO'.ACTIVE_OBJECTCROSSREF': SELECT;
catalog sql object '_SYS_REPO'.PACKAGE_CATALOG': SELECT;
catalog sql object '_SYS_REPO'.ACTIVE_OBJECT_TEXT_CONTENT': SELECT;
catalog sql object '_SYS_REPO'.ACTIVE_CONTENT_TEXT_CONTENT': SELECT;
catalog sql object '_SYS_SECURITY'._SYS_PASSWORD_BLACKLIST': SELECT;
...
}
```

Weitere Ergänzungen können nach Bedarf erfolgen.

7. Zusammenfassung und Übersicht für die Nutzeradministration

Aktivitäten	Erledigt	Offen
SAP Auditor Berechtigungsrollen in Kundennamensraum kopieren und Org-Ebenen sowie spezielle Felder ergänzen.		
Erweiterte Transaktionen für die Berechtigungsrollen (u.a Eintrag „S*“ für Objekt „S_TCODE“) ermöglichen. Die Beschränkung auf Anseh-Funktionalität wird bereits durch vorbereitete Einträge des Feldes „Aktivität“ innerhalb der Audit-Rollen sichergestellt.		
Downloadberechtigung für SAP-Daten prüfen und berücksichtigen (Berechtigung zu Objekt S_GUI).		
Berechtigung zur Pflege von Nutzervorgaben (SU3) prüfen und berücksichtigen.		
Berechtigung zur Nutzung der Variantentechnik, Hintergrundverarbeitung und Job-Steuerung prüfen und berücksichtigen		
Änderungsberechtigung für Tabelle TVARV über Berechtigungsobjekt „S_TABU_NAM“ sicherstellen (OSS 1481950).		
UP- und Downloadberechtigung für Menü-Favoriten prüfen und sicherstellen.		
SAP Benutzer für den Prüfer anlegen		
SAP Auditor Menürollen unverändert der Prüfungskennung zuordnen		
Angepasste SAP Auditor Berechtigungsrollen aus dem Kundennamensraum einzeln oder als Sammelrolle der Prüfungskennung zuordnen		
Prüferkennung den Query-Benutzergruppen /SAPQUERY/AU und /SAPQUERY/AM zuordnen		
HANA-Prüferrolle für Datenbanknutzer einrichten (PUBLIC mit erweiterten PRIVILEGES -Package, System, Application, Object)		
Personalisierte HANA-DB-Nutzerkennung für Revisor anlegen und neue Prüferrolle zuordnen.		
Zugangsdaten (Client, Netz, Windows, SAP, HANA-DB) aufschreiben und mitteilen		

8. Nutzerkennungen und Ansprechpartner

Zum Zeitpunkt der Prüfung müssen eine schriftliche Übersicht mit der SAP-Kennung und deren Passwort sowie eine Aufzeichnung der Zugangskennung für das Netzwerk vorhanden sein.

- SAP System _____
- SAP-Prüfungsmandant _____
- SAP-Nutzerkennung _____
- SAP-Initialpasswort _____
- HANA DB-Nutzerkennung _____
- HANA-DB Initialpasswort _____
- Netz-Zugangskennung _____
- Netz-Passwort _____
- Netzserver _____
- Kontext _____
- Home-Laufwerk _____
- Windows-Nutzer _____
- Windows-Passwort _____

Es wäre günstig, wenn eine kurze Einweisung durch den Systemadministrator erfolgen könnte.

9. Information und Rücksprache

Soweit bestimmte Voraussetzungen nicht erfüllbar sind, bitten wir höflich um eine rechtzeitige Information und Abstimmung.

Roger Odenthal & Partner Unternehmensberatung
Wiener Platz 2
51065 Köln
Telefon: 0221-4921403
Telefax: 0221-4921404
Email: info@roger-odenthal.de
Home: www.roger-odenthal.de

10. Eigene Einrichtungsaktivitäten des SAP-Nutzers (Prüfers)

Nach Einrichtung der Nutzerkennung und erstmaliger Anmeldung auf der SAP-Applikation sind folgende Aktivitäten des SAP-Nutzers (Prüfers) sinnvoll:

- Einrichtung des Druckers im Hinblick auf ausreichende Arbeitspapiere

Innerhalb der Nutzervorgaben (Transaktion SU3) kann über den Reiter „Festwerte“ und der Rubrik „Spoolsteuerung - Ausgabegerät“ ein geeigneter SAP-Standarddrucker oder lokaler Drucker ausgewählt werden.

Beim erstmaligen Druck über diesen Drucker über den Schalter „Eigenschaften“ zur Option „Deckblätter“ wechseln, "Erweiterte Eigenschaften" und dort das „Selektionsdeckblatt“ dauerhaft einstellen.

- Einrichtung von Nutzerparametern

Innerhalb der Nutzervorgaben (Transaktion SU3) können über den Reiter „Parameter“ nutzerbezogene Einstellungen festgelegt werden. Die zu Verfügung stehenden Parameter sind aus der Tabelle „TPARA“ ersichtlich. Sinnvoll sind u.a. die Festlegung der Downloadpfade für Prüfungsergebnisse oder Parameter zur Businessstruktur z.B:

- GR8 C:\Temp (Downloadpfad)
- GR9 C:\Temp (Uploadpfad)
- BUK (Buchungskreis)
- BAR (Belegart)
- GJR (Geschäftsjahr)
- BIL (Bilanz)
- GLN (Ledger)
- Weitere Nutzerparameter

- Konfektionierung der SAP-Oberfläche (bei Zugang über SAP-GUI)

Design, Farben, Schriftarten und -größen sowie Geräusche oder Downloadpfade etc. können seitens des Prüfers direkt über die SAP-GUI eingestellt werden.

