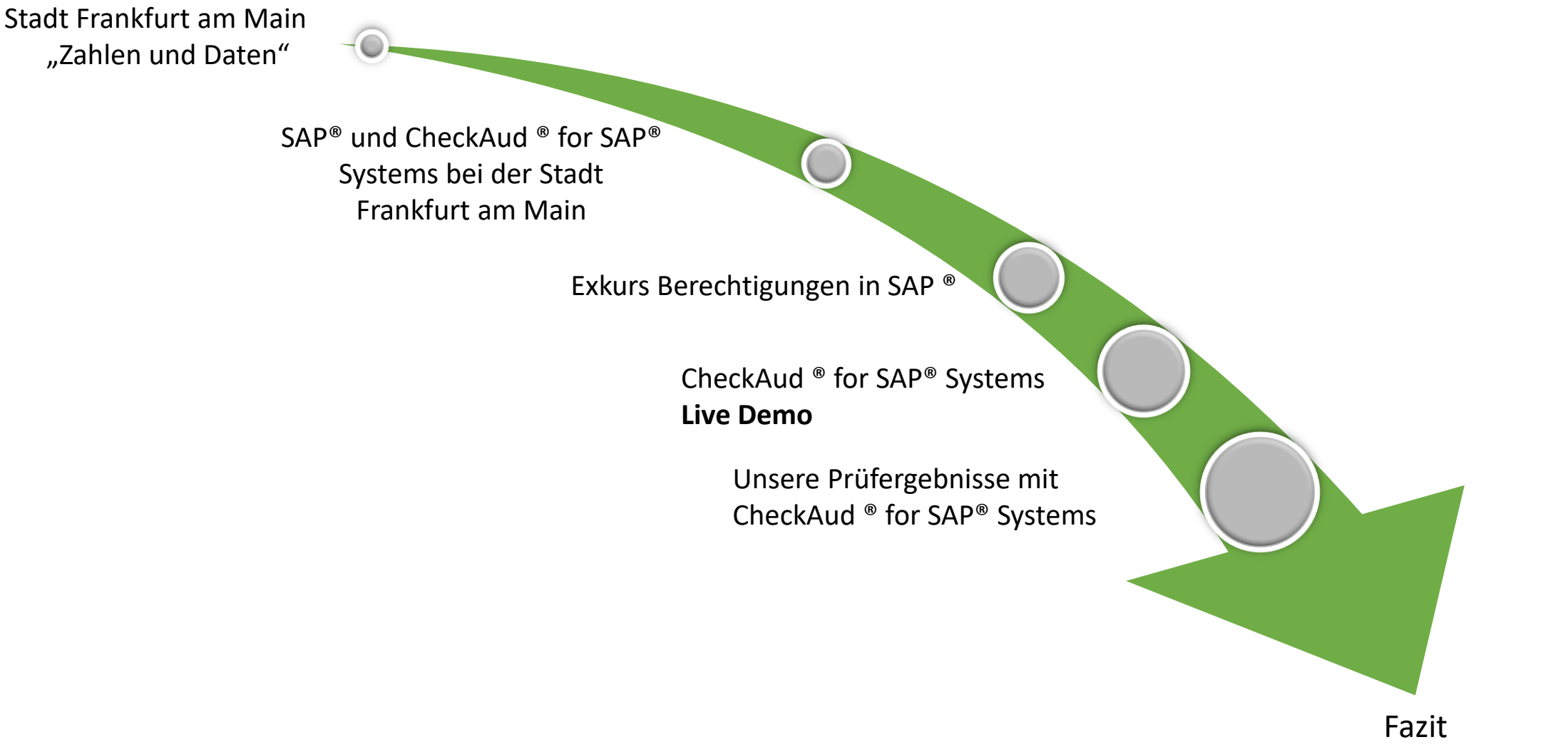
STADT FRANKFURT AM MAIN

CheckAud® for SAP® Systems
Prüfsoftware für SAP® Berechtigungsdaten

Wiener Symposium 2019 der städtischen Kontrolleinrichtungen
22. Mai 2019
„Daten, Fluch oder Segen in der Prüfung“

Agenda


Stadt Frankfurt am Main
„Zahlen und Daten“
SAP® und CheckAud ® for SAP® Systems bei der Stadt Frankfurt am Main
Exkurs Berechtigungen in SAP ®
CheckAud ® for SAP® Systems
Live Demo
Unsere Prüfergebnisse mit CheckAud ® for SAP® Systems
Fazit

Größe

Größte Stadt in Hessen und fünftgrößte in Deutschland
nach Berlin, Hamburg, München und Köln.

Öffentliche Finanzen (IN MIO. €)

Steuereinnahmen	2 345
Schulden	1 512

Bevölkerung

Einwohner zum 18.02.2019	750 000

Wirtschaft

Betriebe	42 666
Kreditinstitute	202

Stadtverwaltung

Mitarbeitende	ca. 13 000
Ämter, Betriebe	62

Quelle: www.stadt-frankfurt.de

Eröffnungsbilanz zum 01. Januar 2007

Vermögen	12,52 Milliarden €
Anlagevermögen	11,8 Milliarden €
Straßen	1145 Km
Grundstücke	44.266
Gebäude	ca. 1800
U-Bahn Gleise	58,6 Km
Palmengarten	c.a. 2500 Pflanzenarten
Zoo	c.a. 4500 Tiere aus 580 Arten
Höchster Buchwert aller Gebäude	Dom 58 Millionen €

Quelle: www.stadt-frankfurt.de

- Einführung von SAP® zum 01.01.2007.

- Aktuell wird SAP® ERP 6.07 auf einem SAP Netweaver 7.40 in einer dreistufigen Systemlandschaft eingesetzt.

- Es kommen folgende Module zum Einsatz:

  BC, CO, EC-PCA, FI, FI-AA, IM, MM, PM, PSCD, PSM, SD.

- Zusätzlich wird DZ-Kommunalmaster® SteuernAbgaben (KM-StA) eingesetzt. KM-StA ist ein vollintegriertes Veranlagungsverfahren auf Basis von SAP® ERP / PSCD.

- Für den Konzernabschluss wird das Modul SEM-BW 7.47 auf einem SAP® BI 7.0 System in einer dreistufigen Systemlandschaft eingesetzt.

- Benutzeranzahl: ca. 1.200 im produktiven ERP System
  ca. 80 im produktiven BW System

- Anzahl der Rollen: ca. 1.600 im produktiven ERP System
  ca. 260 im produktiven BW System

- Bis Ende 2011 wurden die Berechtigungen manuell mit den Auswertungsmöglichkeiten von SAP® geprüft.

- Kauf der Software CheckAud® for SAP® Systems im Januar 2012.

- Erstprüfung durch die Fa. IBS Schreiber GmbH im März 2012 für die Module BC und FI im ERP System, sowie eine Erstprüfung des SAP® BW Systems.

STADT FRANKFURT AM MAIN

Benutzer- Berechtigungskonzept

- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Authentizität
- Verbindlichkeit

GemHVO

BSI

GoBD

GemKVO

EU-DSGVO

HGO

RO

HGB

Ordnungsmäßigkeit-Zweckmäßigkeit-Wirtschaftlichkeit

Benutzer- Berechtigungskonzept

Beispiel: Kreditorenstammsatz anzeigen

Berechtigungsobjekt	Berechtigungsfeld	Wert Berechtigung	Bedeutung	Transaktion
S_TCODE				FK03
F_LFA1_APP	ACTVT APPKZ	03 F	Aktivität = Anzeigen Antragsberechtigung = F	
F_LFA1_BUK	ACTVT BUKRS	03 z.B. 1000	Aktivität = Anzeigen Buchungskreis = 1000	
F_LFA1_GEN	ACTVT	03	Aktivität = Anzeigen	
F_FNA1_GRP	ACTVT KTOKK	03 z.B. 0001	Aktivität = Anzeigen Kontengruppe = 0001	

Benutzer- Berechtigungskonzept

Kritische Sammelprofile:

SAP_ALL[1]	S_A.SYSTEM
SAP_NEW[2]	F_BUCH_ALL
S_A.ADMIN[3]	Z_ANWEND
S_A.DEVELOP	

Benutzer- Berechtigungskonzept

Gesetzeskritische Berechtigungen:

Löschen von Tabellenänderungsprotokollen	10 Jahre Aufbewahrungspflicht § 257 HGB
Löschen von Änderungsbelegen	10 Jahre Aufbewahrungspflicht § 257 HGB und Radierverbot § 239 HGB
Löschen von Versionen	10 Jahre Aufbewahrungspflicht § 257 HGB
Debuggen mit der Möglichkeit zum Ändern im Hauptspeicher	Radierverbot § 239 Abs. 3 HGB
ABAB-Quelltexte über RFC installieren und deren ungeprüfte Ausführung	Radierverbot § 239 Abs. 3 HGB

Warum die Analyse der SAP® Berechtigungen komplex ist?

Ein Beispiel:

- Änderungen an den Tabellen im SAP® System müssen protokolliert werden und werden in den Tabellenänderungsprotokollen aufgezeichnet.

- Diese dürfen nicht gelöscht werden.

- Ein Prüfungsansatz ist also die Frage,
  wer kann die Tabellenänderungsprotokolle löschen?

Keiner?

Wie kann ich die Tabellenänderungsprotokolle löschen?

➢ Dies kann mit dem SAP®-Standardreport RSTBPDEL erfolgen oder über die Transaktion SCU3.

Welche Berechtigungsobjekte werden benötigt?

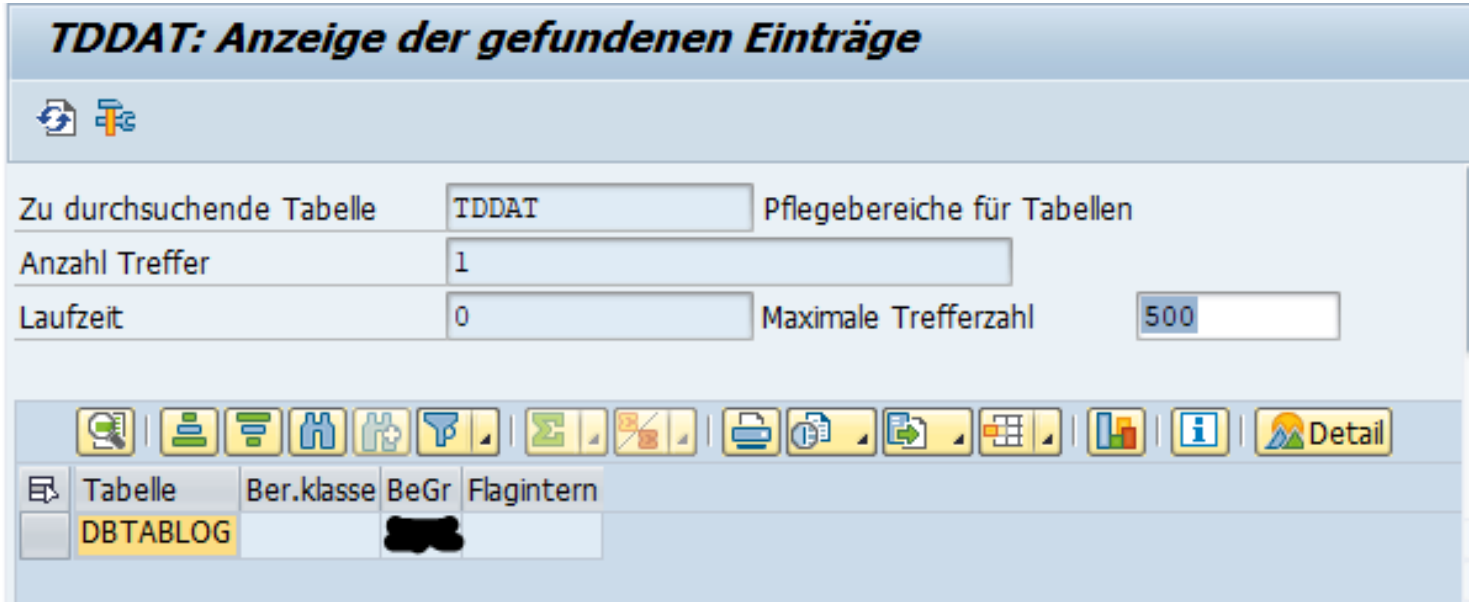
Berechtigungsobjekt	Berechtigungsfeld	Wert Berechtigung	Bedeutung	Transaktion
S_TCODE				SCU3
S_TABU_DIS	ACTVT DICBERCLS	02 SA	Aktivität = Ändern Tabellenberechtigungsgruppe = SA	
S_TABU_CLI	CLIIMAINT	X	erlaubt: Pflege mandanten-unabhängiger Tabellen	

…oder…

Berechtigungsobjekt	Berechtigungsfeld	Wert Berechtigung	Bedeutung	Transaktion
S_TCODE				SCU3
S_TABU_NAM	ACTVT TABLE	02 DBTABLOG	Aktivität = Ändern Tabellenname = DBTABLOG	
S_TABU_CLI	CLIIMAINT	X	erlaubt: Pflege mandanten-unabhängiger Tabellen	

Aber befindet sich die Tabelle überhaupt in dieser Berechtigungsgruppe?

- Im SAP Standard befindet sie sich in der Tabellenberechtigungsgruppe „SA“…
- Weitere Prüfung der Berechtigungsgruppe für die Tabelle DBTABLOG ist erforderlich…



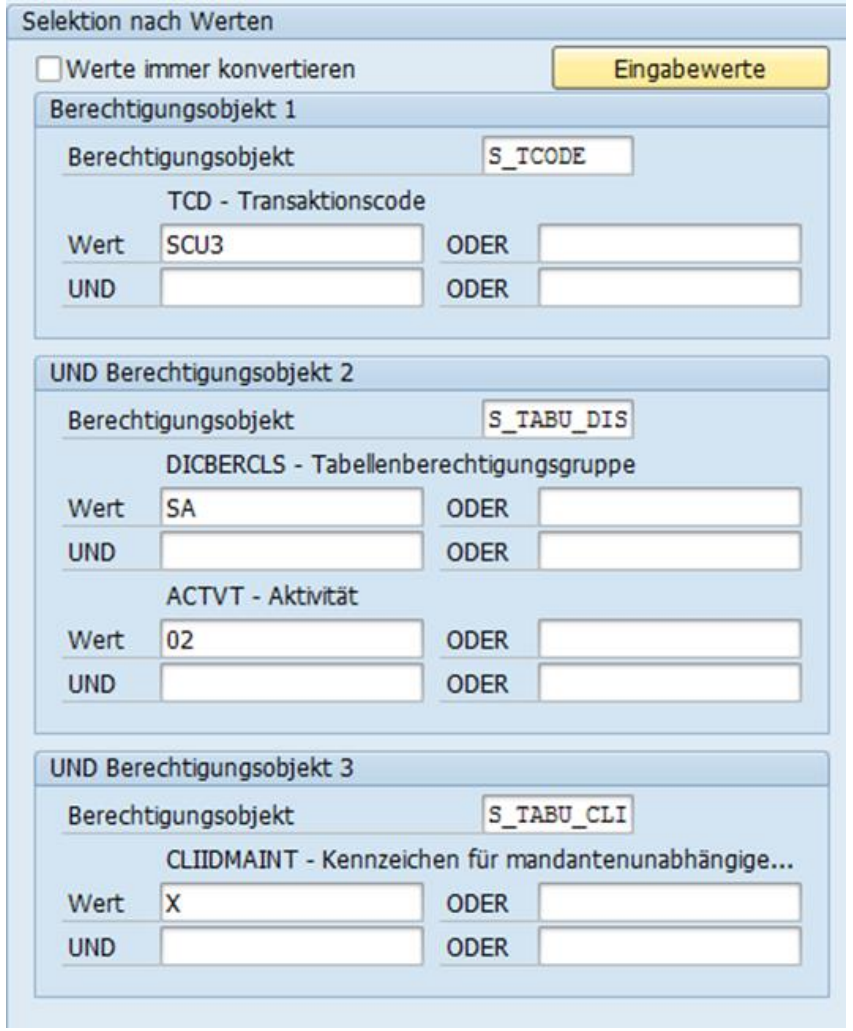
Kann ich diese Frage mit den Auswertungsmöglichkeiten im SAP® System beantworten?

J E I N

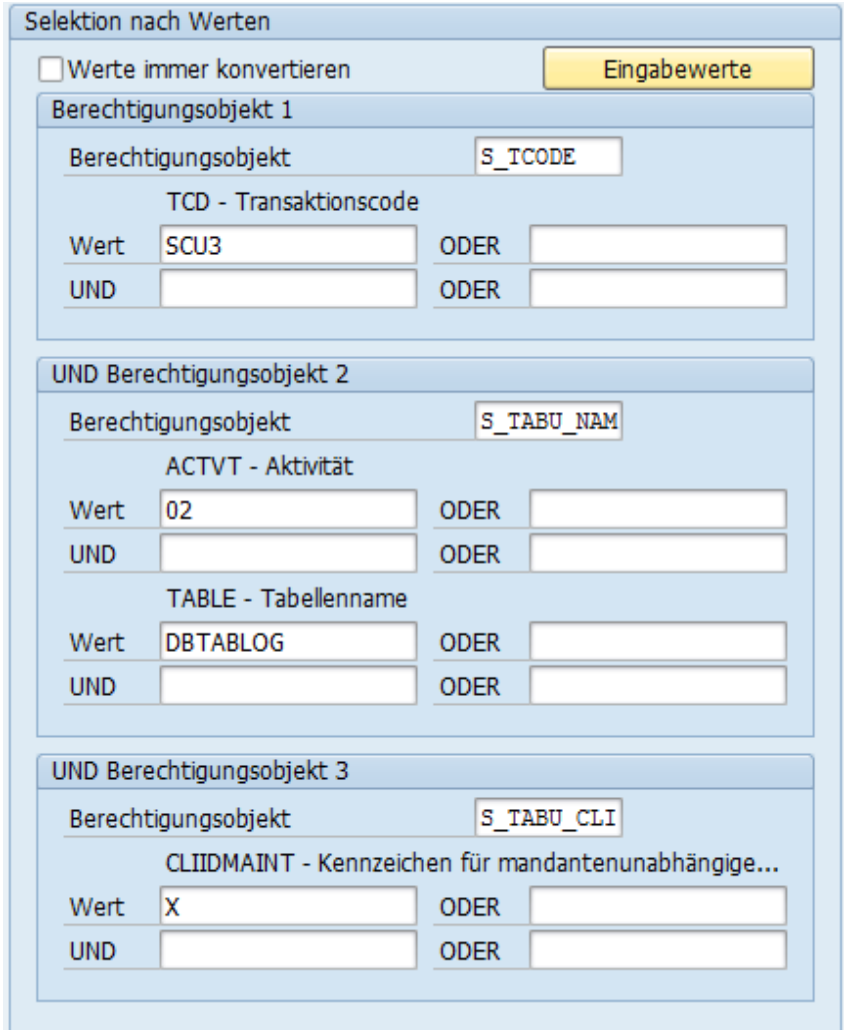
Das Infosystem (Transaktion SUIM) bietet u. a. die Auswertung „Benutzer nach komplexen Selektionskriterien“

Hier gibt es Einschränkungen:

- Maximal 4 Berechtigungsobjekte in einer UND – Verknüpfung
- Keine ODER – Verknüpfung möglich
- Prüfung der tatsächlichen Berechtigungsgruppe erfolgt hier nicht



- Fragestellung kann nicht direkt im SAP® System beantwortet werden
- Die Abfrage muss auf mehrere Auswertungen aufgeteilt werden
- Um die Ergebnisse weiter bearbeitet zu können, müssen diese exportiert werden
- Es können keine Abfragen hinterlegt werden
- Alle Abfragen sind wieder neu einzugeben
- Die Ergebnisse der beiden Abfragen müssen zusammengeführt und gegebenenfalls um Duplikate bereinigt werden.



Darüber hinaus gibt es noch ein mehrfaches an relevanten Prüfungsfragen zur Berechtigungsvergabe in einem SAP® System.

Der Aufwand für die Prüfung vervielfacht sich dementsprechend.

Einfache Frage, einfache Antwort?
Leider nicht!

- Diese Prüfung ist zeitaufwendig.
- Die Parameter der Abfragen können nicht gespeichert werden.
- Eine regelmäßige Überprüfung ist nur mit manuellem Aufwand möglich.

Und was nun?

Datenanalyse!

Datenanalyse als Lösung?

- Alle Informationen zu den Benutzern und Berechtigungen werden in SAP in Tabellen gespeichert, theoretisch liegen damit die Voraussetzungen für eine Datenanalyse vor.

- Um diesen Datenschatz zu heben, müssen diese Tabellen identifiziert, exportiert und ausgewertet werden können.

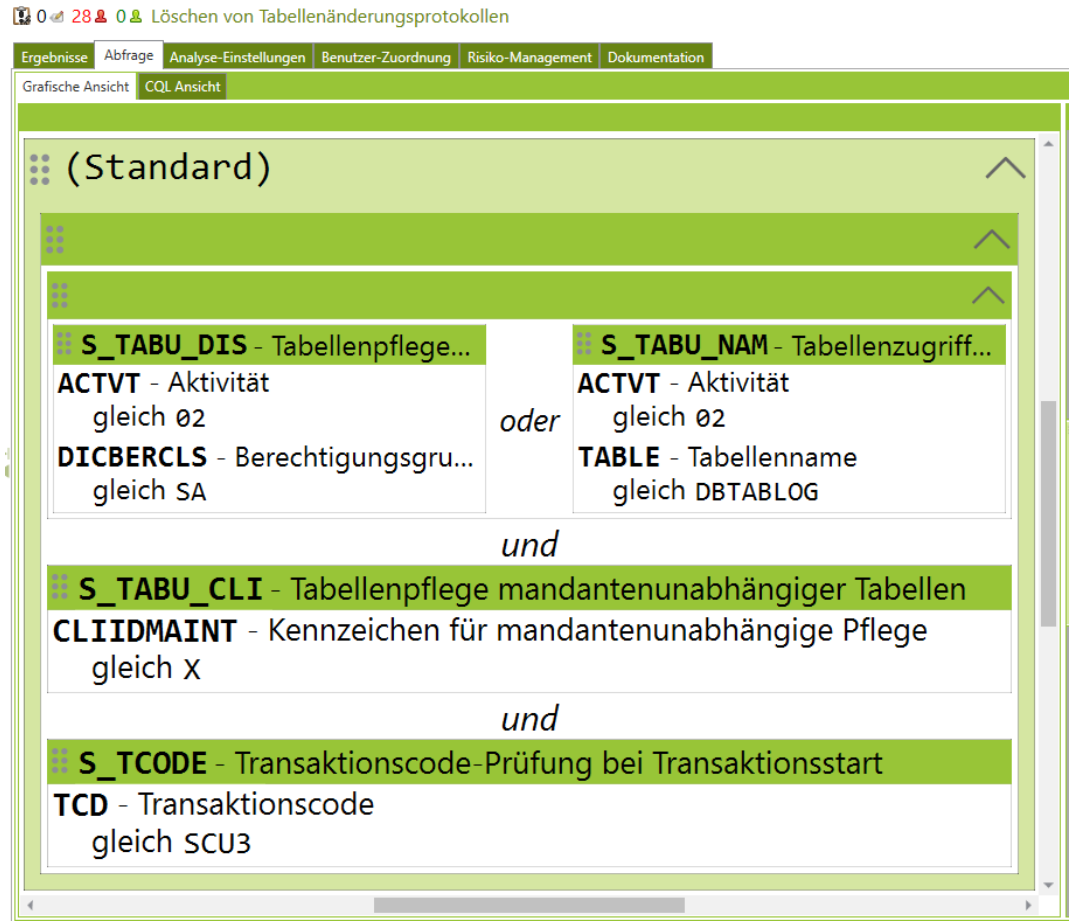
- Nach einer Markterkundung haben wir die für uns passende Softwarelösung zum Prüfen von SAP Berechtigungen gefunden, welche wir Ihnen nun kurz vorstellen wollen.

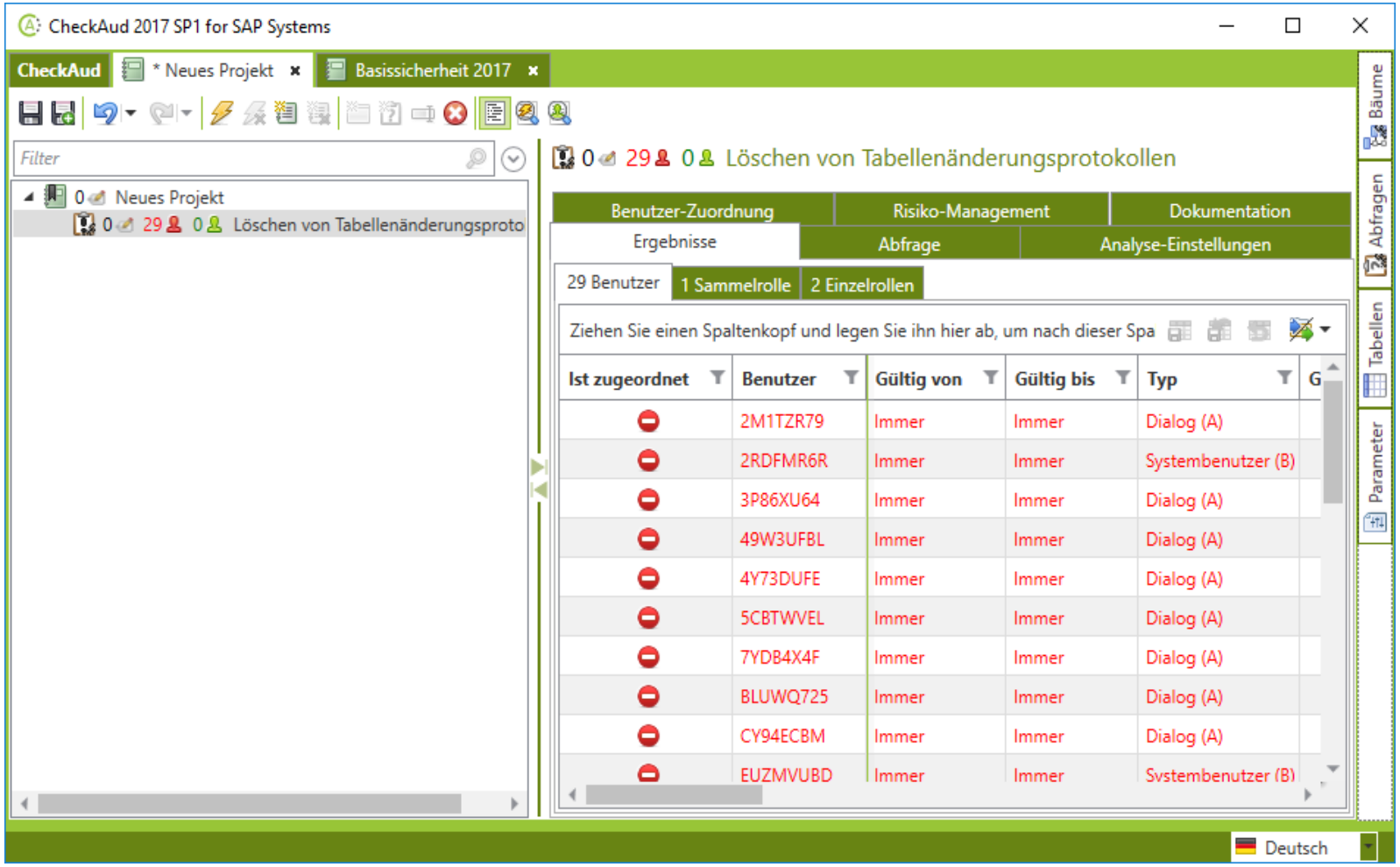
Live Demo

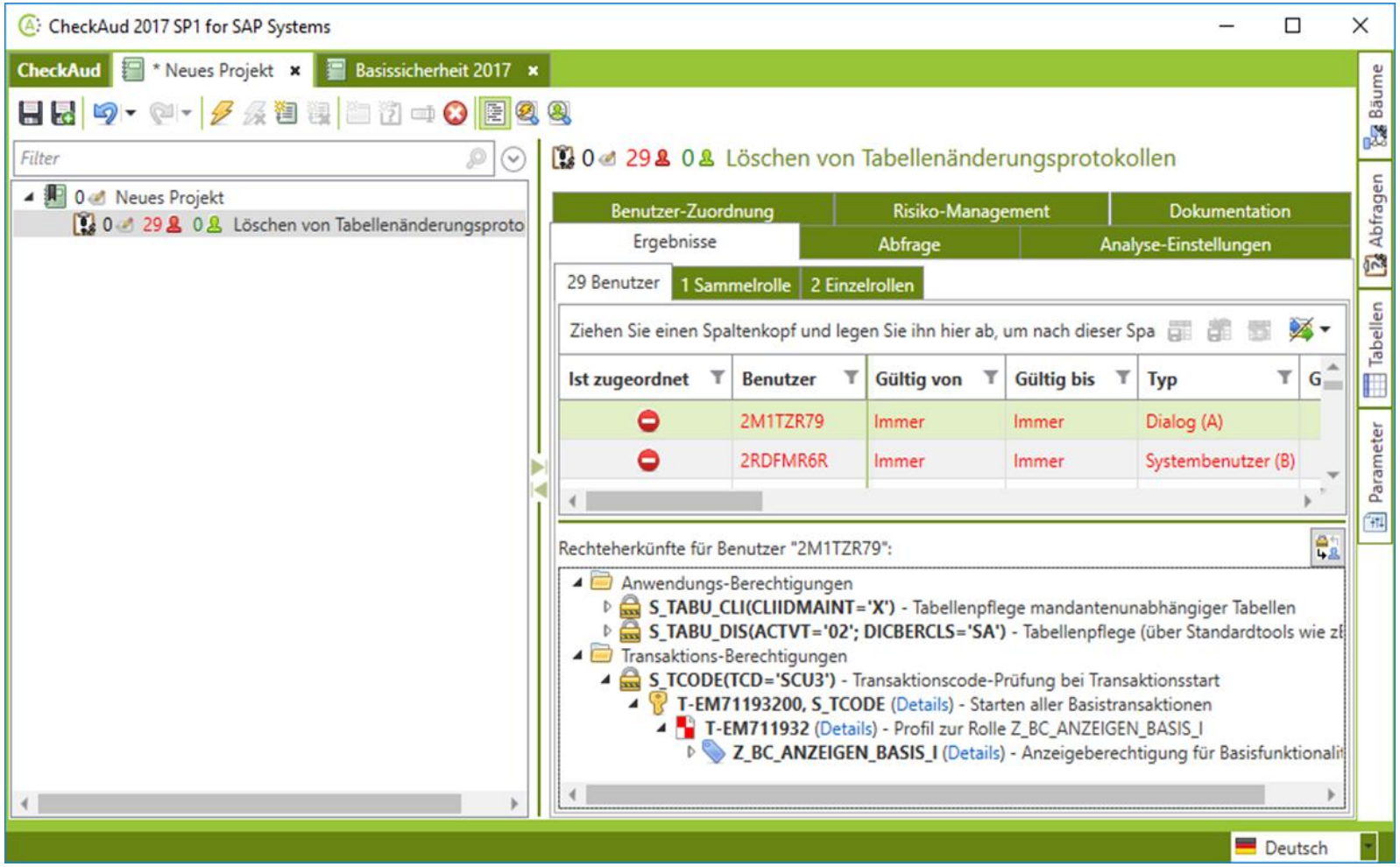
So sieht zum Beispiel unsere Fragestellung in der Prüfsoftware CheckAud® aus:

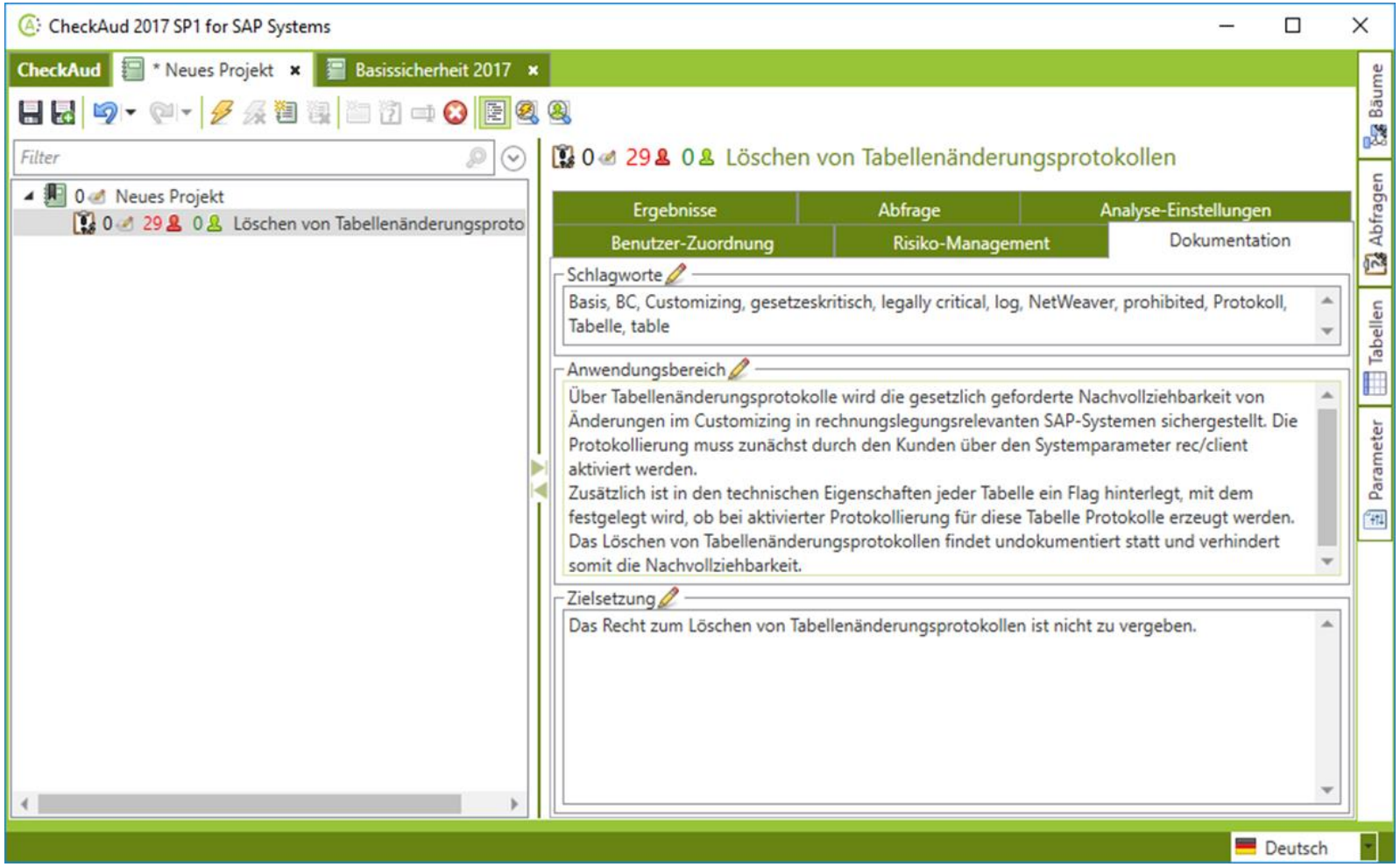
Grafische Ansicht | CQL Ansicht

```
{
 (
  (
   S_TABU_DIS(ACTVT = '02', DICBERCLS = 'SA')
   or
   S_TABU_NAM(ACTVT = '02', TABLE = 'DBTABLOG')
  )
  and
  S_TABU_CLI(CLIIDMAINT = 'X')
  and
  S_TCODE(TCD = 'SCU3')
 )
}
```

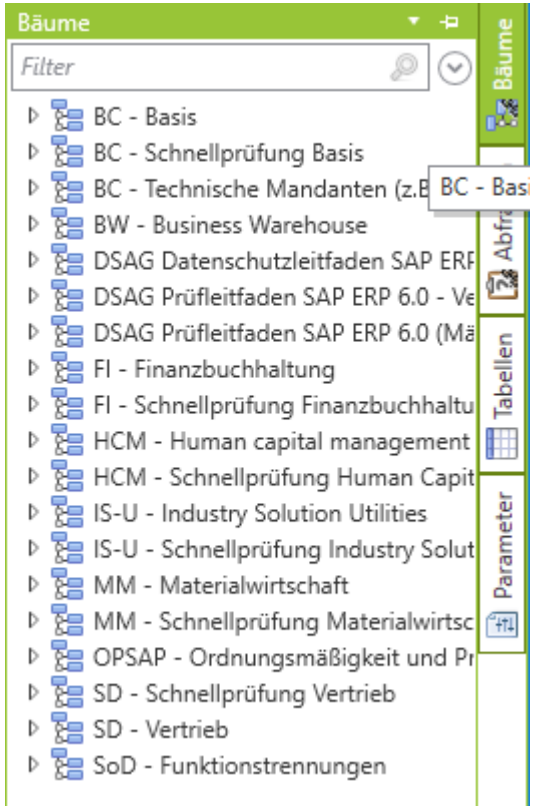



CheckAud 2017 SP1 for SAP Systems
CheckAud
* Neues Projekt
Basissicherheit 2017
Filter
0 Neues Projekt
0 29 0 Löschen von Tabellenänderungsproto
0 29 0 Löschen von Tabellenänderungsprotokollen
Benutzer-Zuordnung
Risiko-Management
Dokumentation
Ergebnisse
Abfrage
Analyse-Einstellungen
29 Benutzer
1 Sammelrolle
2 Einzelrollen
Ziehen Sie einen Spaltenkopf und legen Sie ihn hier ab, um nach dieser Spa
Ist zugeordnet
Benutzer
Gültig von
Gültig bis
Typ
2M1TZR79 Immer Immer Dialog (A)
2RDFMR6R Immer Immer Systembenutzer (B)
3P86XU64 Immer Immer Dialog (A)
49W3UFBL Immer Immer Dialog (A)
4Y73DUFE Immer Immer Dialog (A)
5CBTWVEL Immer Immer Dialog (A)
7YDB4X4F Immer Immer Dialog (A)
BLUWQ725 Immer Immer Dialog (A)
CY94ECBM Immer Immer Dialog (A)
EUZMVUBD Immer Immer Systembenutzer (B)
Bäume
Abfragen
Tabellen
Parameter
Deutsch


CheckAud 2017 SP1 for SAP Systems
CheckAud
* Neues Projekt
Basissicherheit 2017
Filter
0 Neues Projekt
0 29 0 Löschen von Tabellenänderungsproto
0 29 0 Löschen von Tabellenänderungsprotokollen
Benutzer-Zuordnung
Risiko-Management
Dokumentation
Ergebnisse
Abfrage
Analyse-Einstellungen
29 Benutzer
1 Sammelrolle
2 Einzelrollen
Ziehen Sie einen Spaltenkopf und legen Sie ihn hier ab, um nach dieser Spa
Ist zugeordnet
Benutzer
Gültig von
Gültig bis
Typ
2M1TZR79
Immer
Immer
Dialog (A)
2RDFMR6R
Immer
Immer
Systembenutzer (B)
Rechteherkünfte für Benutzer "2M1TZR79":
Anwendungs-Berechtigungen
S_TABU_CLI(CLIIDMAINT='X') - Tabellenpflege mandantenunabhängiger Tabellen
S_TABU_DIS(ACTVT='02'; DICBERCLS='SA') - Tabellenpflege (über Standardtools wie z
Transaktions-Berechtigungen
S_TCODE(TCD='SCU3') - Transaktionscode-Prüfung bei Transaktionsstart
T-EM71193200, S_TCODE (Details) - Starten aller Basistransaktionen
T-EM711932 (Details) - Profil zur Rolle Z_BC_ANZEIGEN_BASIS_I
Z_BC_ANZEIGEN_BASIS_I (Details) - Anzeigeberechtigung für Basisfunktionali
Bäume
Abfragen
Tabellen
Parameter
Deutsch


CheckAud 2017 SP1 for SAP Systems
CheckAud
* Neues Projekt
Basissicherheit 2017
Filter
0 Neues Projekt
0 29 0 Löschen von Tabellenänderungsproto
0 29 0 Löschen von Tabellenänderungsprotokollen
Ergebnisse
Abfrage
Analyse-Einstellungen
Benutzer-Zuordnung
Risiko-Management
Dokumentation
Schlagworte
Basis, BC, Customizing, gesetzeskritisch, legally critical, log, NetWeaver, prohibited, Protokoll, Tabelle, table
Anwendungsbereich
Über Tabellenänderungsprotokolle wird die gesetzlich geforderte Nachvollziehbarkeit von Änderungen im Customizing in rechnungslegungsrelevanten SAP-Systemen sichergestellt. Die Protokollierung muss zunächst durch den Kunden über den Systemparameter rec/client aktiviert werden.
Zusätzlich ist in den technischen Eigenschaften jeder Tabelle ein Flag hinterlegt, mit dem festgelegt wird, ob bei aktivierter Protokollierung für diese Tabelle Protokolle erzeugt werden.
Das Löschen von Tabellenänderungsprotokollen findet undokumentiert statt und verhindert somit die Nachvollziehbarkeit.
Zielsetzung
Das Recht zum Löschen von Tabellenänderungsprotokollen ist nicht zu vergeben.
Bäume
Abfragen
Tabellen
Parameter
Deutsch

Die in der Prüfsoftware CheckAud® for SAP® Systems bereits vordefinierten Abfragen sind zusätzlich auch thematisch zusammen gefasst:



Und was nun?

Der Tabellenzugriff und die Tabellenpflege für die Tabellenänderungsprotokolle (Tabelle DBTABLOG) wurde aufgrund unserer Prüfung im SAP® System der Stadt Frankfurt am Main zusätzlich abgesichert.

Es wurde eine eigene Berechtigungsgruppe eingerichtet und die Tabelle DBTABLOG dieser Berechtigungsgruppe zugewiesen.

Der direkte Tabellenzugriff und die Tabellenpflege für diese Berechtigungsgruppe wurde nicht vergeben.

Mit Hilfe der Prüfsoftware CheckAud® for SAP® Systems wird dies monatlich überprüft.

CheckAud® for SAP® Systems wurde mit der Zielsetzung entwickelt, das Berechtigungskonzept transparent abzubilden und auf einfache und komfortable Weise prüfbar zu machen.

Die gesamten Zugriffsrechte werden in verschiedenen Baumstrukturen dargestellt. Z.B. werden alle Profile zu den Benutzern angezeigt, nach Wahl bis hinunter zu den Objekten mit den Feldinhalten. Des Weiteren sind alle Übersichten auch in tabellarischer Form möglich, z.B. eine Tabelle mit allen Benutzern und allen Eigenschaften. Hier können dann auch beliebige Filter gesetzt werden, z.B. können nur die Benutzer angezeigt werden, die seit einem bestimmten Zeitraum (z.B. 90 Tage) nicht mehr angemeldet waren.

Alle Ergebnisse können jederzeit in Berichtsform abgespeichert werden.

Ein Hauptaugenmerk von CheckAud® for SAP® Systems liegt in der Auswertung von kritischen Berechtigungen. Hier werden grundsätzlich zwei verschiedene Arten von kritischen Berechtigungen unterschieden:

Berechtigungsobjekte, die an sich als kritisch anzusehen sind
(z.B. S_DEVELOP für die Entwicklungsumgebung)

Berechtigungsobjekte, die erst dann kritisch werden, wenn sie in Kombination mit anderen Berechtigungsobjekten vergeben werden (Beispiel: wer darf Kreditorenstammdaten anlegen, für diese dann Belege buchen und die Zahlungsläufe durchführen).

Beide Arten von kritischen Berechtigungen sind mit CheckAud® for SAP® Systems komfortabel darstellbar.

In CheckAud® for SAP® Systems wird eine große Liste von Standardberichten zur Verfügung gestellt, welche die häufigsten Fragestellungen an ein SAP®-System abdecken, z.B.

Welche Benutzer waren noch nie angemeldet?
Welche Benutzer sind durch einen Administrator gesperrt?
Haben die Sonderbenutzer noch ihr Standardkennwort?
Gibt es Benutzer mit Initialkennwort?
Benutzer mit kritischen Profilen (SAP_ALL, S_A.SYSTEM, Z_ANWEND, ...)
Benutzer mit der Komplettberechtigung zur Berechtigungsverwaltung
Benutzer mit Entwicklungsberechtigungen
u.v.a.m.

Benötigte Rechte im SAP®-System

Die Anmeldung über das Scan-Modul an das SAP®-System erfolgt über die RFC Schnittstelle.

Hierfür wird ein Benutzerkonto (Systembenutzer) mit Berechtigungen für den Aufruf von Funktionsbausteinen, Berechtigungsobjekt S_RFC (Remote Function Call), in Verbindung mit Berechtigungen zum Lesen von Tabellengruppen, S_TABU_DIS (Tabellenpflege), oder einzelnen Tabellen, S_TABU_NAM (Tabellenpflege), benötigt.

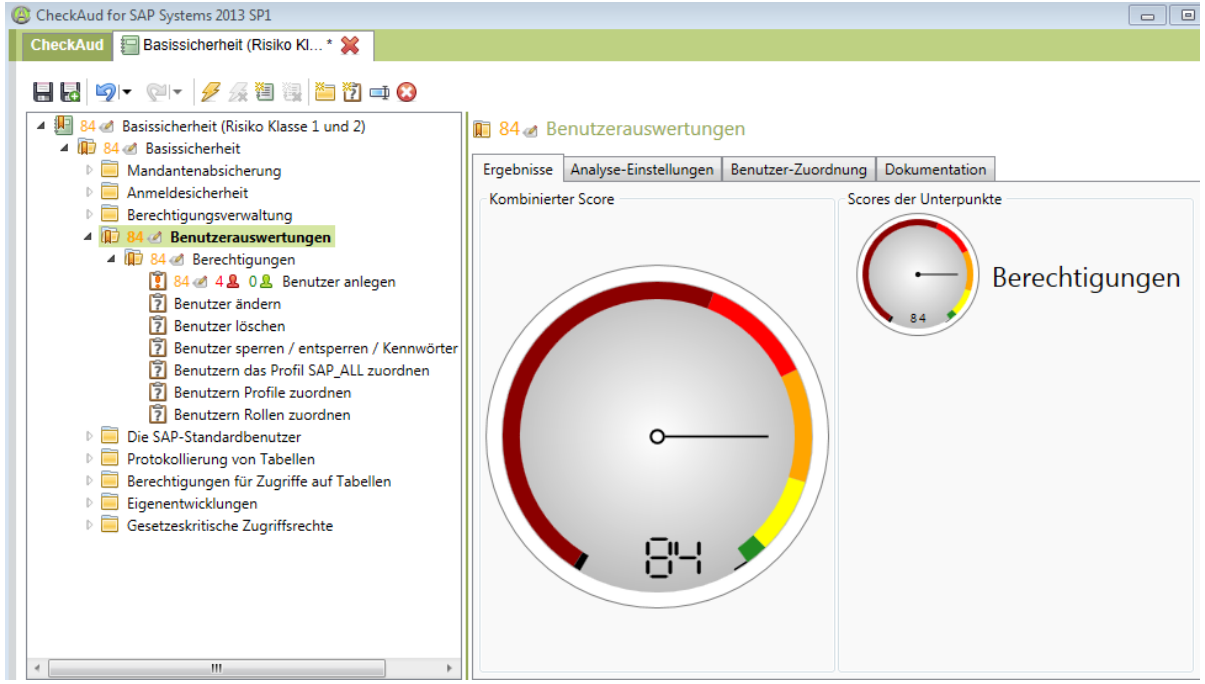
Die detaillierten Berechtigungen sind in der Dokumentation zum Programm CheckAud ® for SAP® Systems beschrieben.

- Die Analyse mit CheckAud® for SAP® Systems bedeutet nicht bei jedem Treffer, dass eine fehlerhafte Vergabe von Berechtigungen vorliegt.

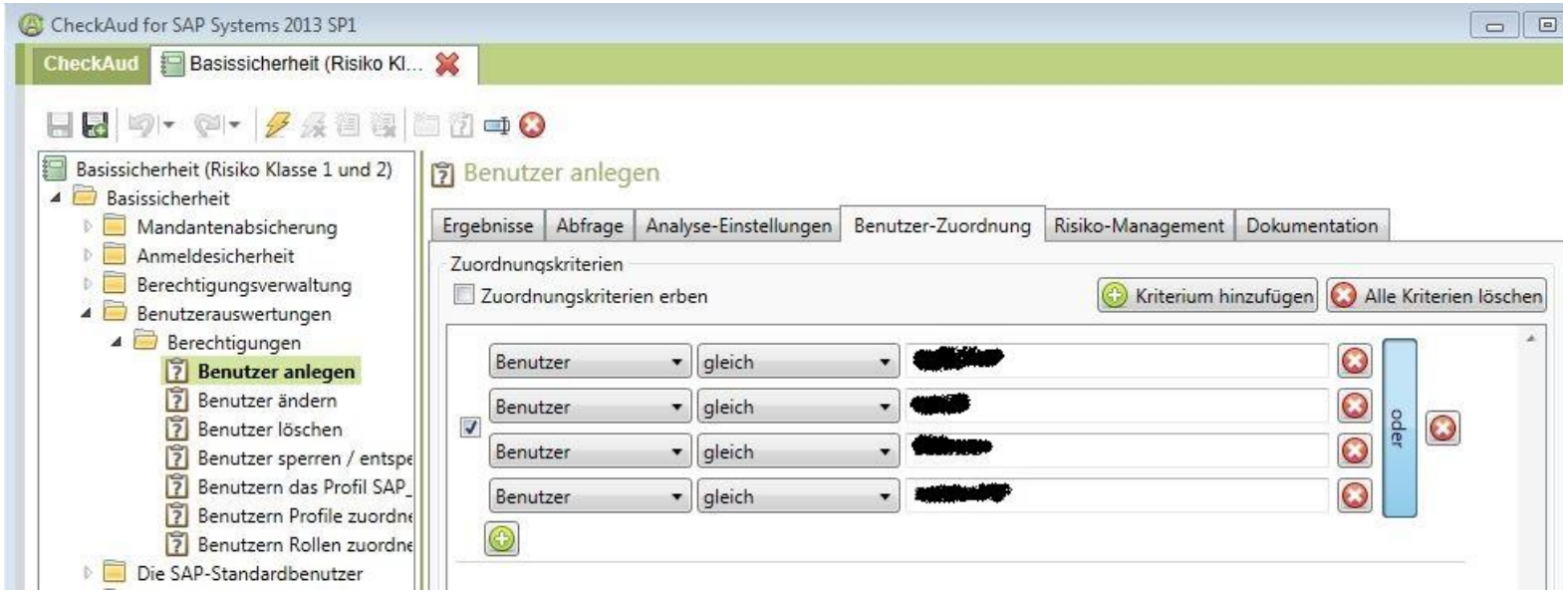
- Kritische Berechtigungen können auch „zu recht“ vergeben werden.
  Zum Beispiel „Benutzer anlegen“.

- Hier sind vier Personen mit der kritischen Berechtigung gefunden worden:

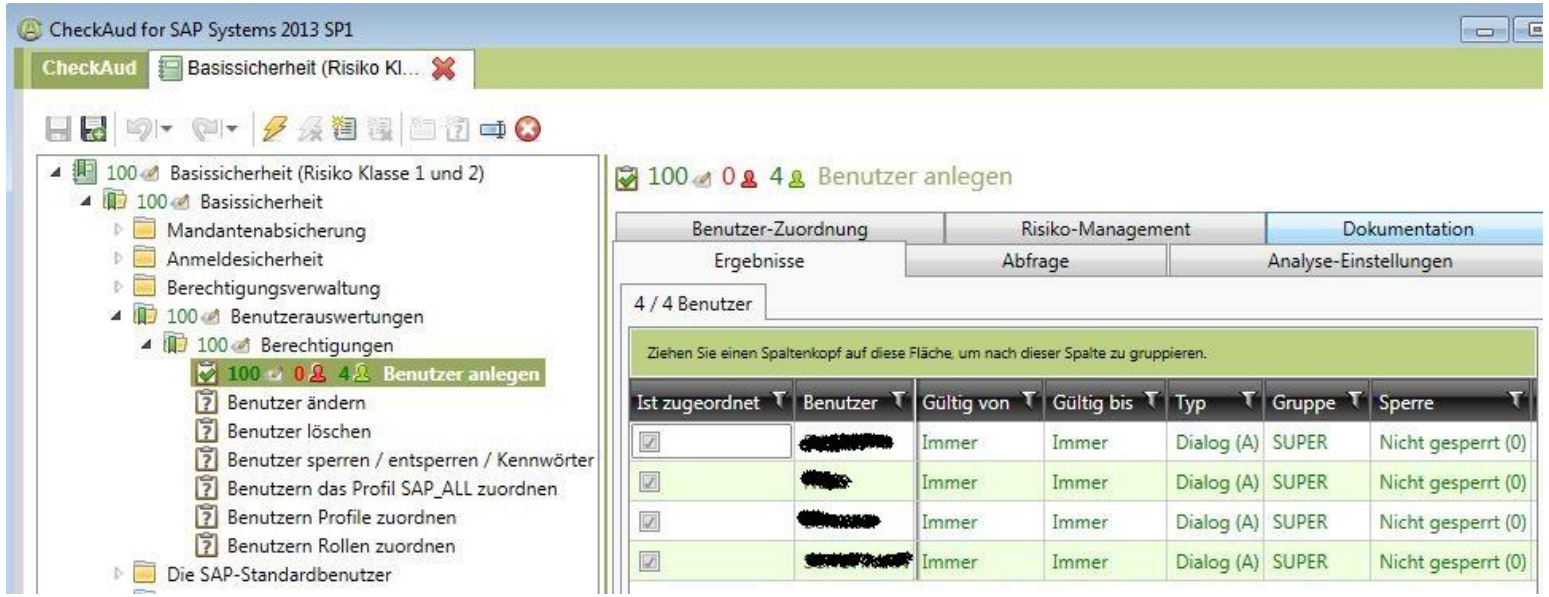
- Hierbei handelt es sich jedoch um Mitarbeiter der Basisadministration, die diese kritische Berechtigung für Ihre Arbeit benötigen. Trotzdem wird das Ergebnis negativ dargestellt. In der sogenannten Tacho – Anzeige wird der Wert 84 (orange) angezeigt.



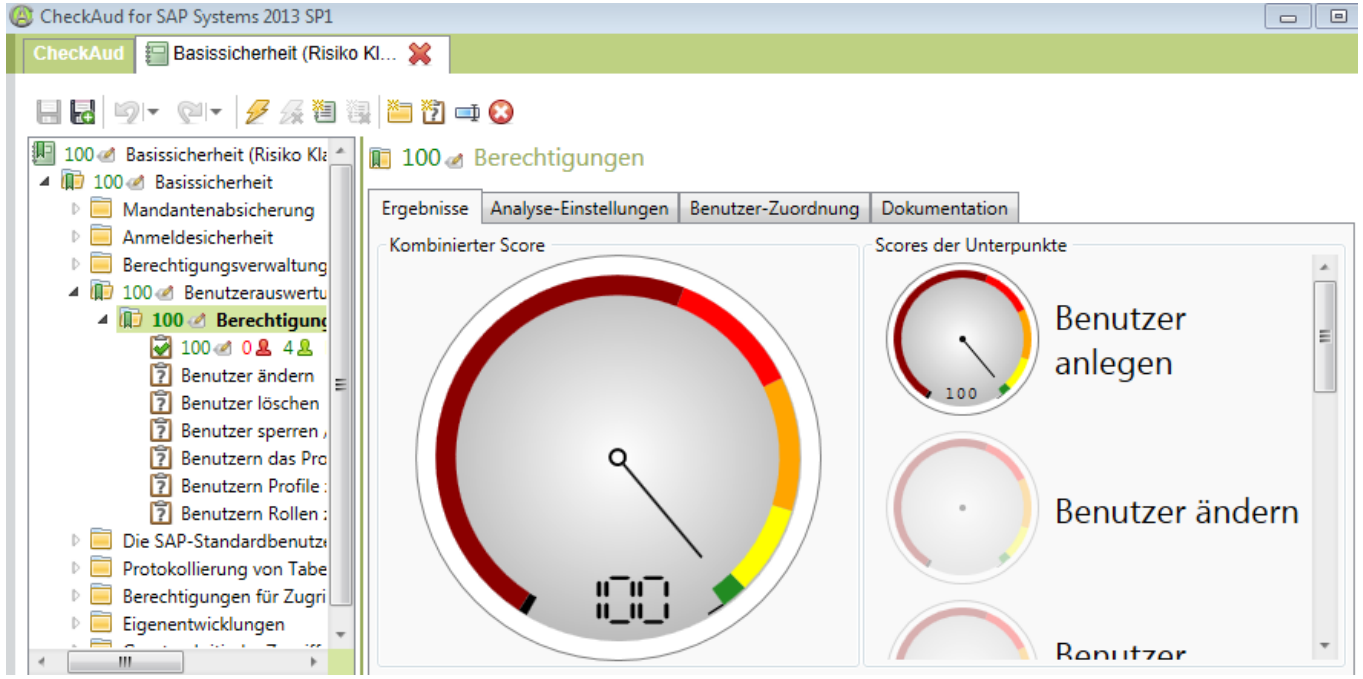
- Die Vergabe von kritischen Berechtigungen kann als „berechtigt“ oder „nicht berechtigt“ definiert werden. Hierzu kann eine Benutzer-Zuordnung für „berechtigte“ Personen in CheckAud® for SAP® Systems hinterlegt werden.



- Die Analyse der kritischen Berechtigung zeigt nun als Ergebnis weiterhin vier Treffer an, weist diese aber nun als „berechtigte“ Benutzer aus. Es werden 0 Benutzer rot und 4 Benutzer grün angezeigt.



- Bei einer regelmäßigen z. B. monatlichen Überwachung können Veränderungen zum Soll direkt erkannt werden. Das Analyseergebnis wird nun trotz vier gefundenen Benutzern in der Tacho - Anzeige als Wert 100 (im grünen Bereich) angezeigt.



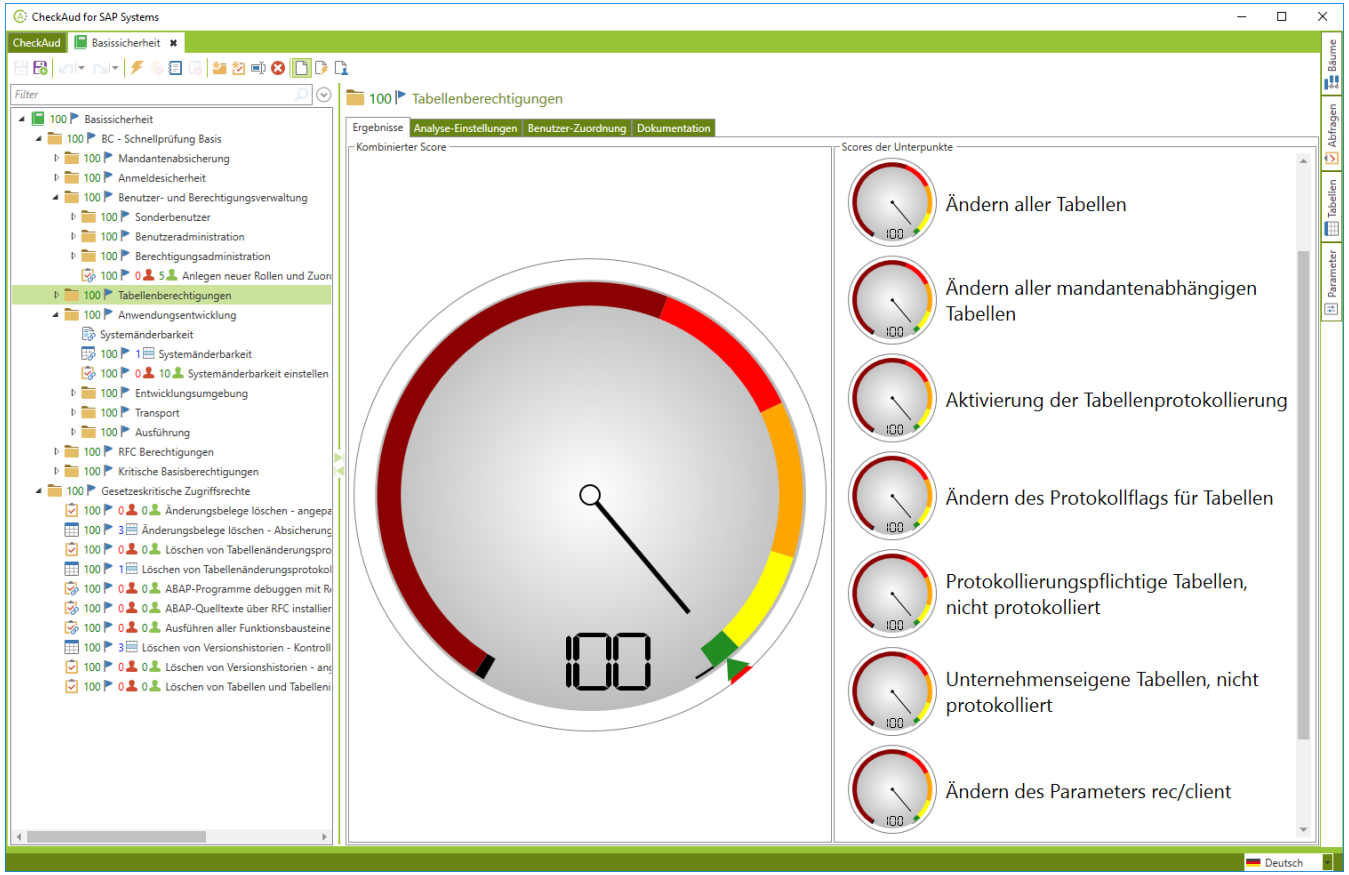
- Das Ergebnis der Erstprüfung für den Bereich BC umfasste 38 kritische Berechtigungen:

Rsk.	Berechtigung:	01.03.12
1	Anlegen neuer Mandanten	42
1	Ändern der Einstellungen bestehender Mandanten	54
1	Systemänderbarkeit einstellen	44
1	Ändern der Anmeldeparameter	28
2	Ändern der Tabelle USR40 (verbotene Kennwörter)	54
2	Sperren des Systems gegen Anmeldungen	44
2	Anlegen neuer Rollen	34
2	Ändern bestehender Rollen	35
2	Anlegen neuer Rollen und Zuordnen zu Benutzern	27
1	Allen Benutzern alle Rollen zuordnen	29
1	Ändern der Prüfkennzeichen zu Berechtigungsobjekten	17
1	Deaktivieren von Berechtigungsobjekten	5
2	Benutzer anlegen	36
2	Benutzer ändern	36
2	Benutzer löschen	36
2	Benutzer sperren / entsperren / Kennwörter vergeben	36
1	Benutzern das Profil SAP_ALL zuordnen	28
2	Benutzern Profile zuordnen	30
2	Benutzern Rollen zuordnen	29
1	Aufruf des Reports RSUSR003	102
1	Benutzer SAP* löschen	36
1	Ändern des Parameters rec/client	28
1	Ändern des Parameters RECCLIENT im Transportverbund	45
2	Ändern des Protokollflags für Tabellen	16
1	Löschen von Tabellenänderungsprotokollen	42
2	Ändern aller mandantenabhängigen Tabellen	80
2	Ändern aller Tabellen	54
2	Lesen aller Tabellen	152
2	ABAP - Programme anlegen	29
2	ABAP - Programme ändern	35
1	Systemänderbarkeit einstellen und ABAPs anlegen oder ändern (ab 7.0)	29
1	Änderungsbelege löschen	8
1	Löschen von Tabellenänderungsprotokollen	42
1	ABAP - Programme debuggen mit Replace	8
1	ABAP - Quelltexte über RFC installieren und ausführen (ab 7.0)	29
1	Ausführen aller Funktionsbausteine	35
1	Versionen löschen	114
	(Neue Abfrage ab 01.01.2013)	
	Summe:	**1528**

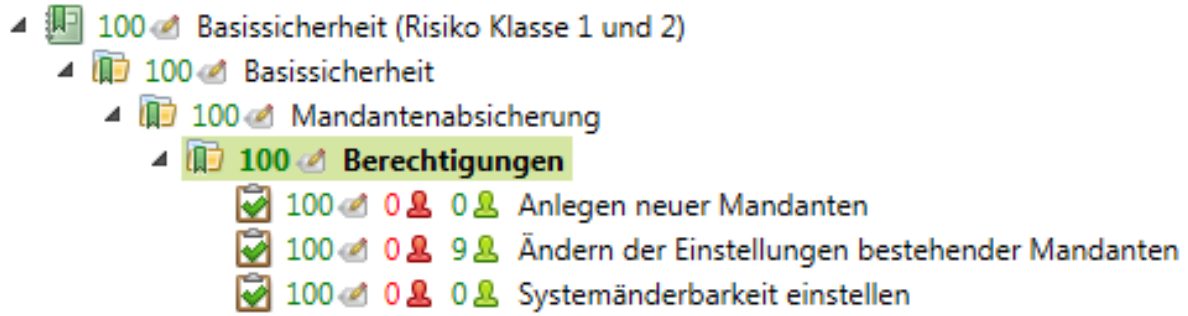
- In Zusammenarbeit mit der SAP Basisadministration wurden die kritischen Berechtigungen angepasst.
- Die Anzahl der Benutzer mit kritischen Berechtigungen konnte innerhalb eines Jahres von 1528 auf 209 reduziert werden.
- Zusätzlich wurden weitere kritische Einstellungen identifiziert und korrigiert.

Erl.	Rsk.	Berechtigung:	01.03.12	31.01.13
X	1	Anlegen neuer Mandanten	42	2
X	1	Ändern der Einstellungen bestehender Mandanten	54	11
X	1	Systemänderbarkeit einstellen	44	2
X	1	Ändern der Anmeldeparameter	28	11
X	2	Ändern der Tabelle USR40 (verbotene Kennwörter)	54	11
X	2	Sperren des Systems gegen Anmeldungen	44	2
X	2	Anlegen neuer Rollen	34	5
X	2	Ändern bestehender Rollen	35	9
X	2	Anlegen neuer Rollen und Zuordnen zu Benutzern	27	5
X	1	Allen Benutzern alle Rollen zuordnen	29	2
X	1	Ändern der Prüfkennzeichen zu Berechtigungsobjekten	17	2
X	1	Deaktivieren von Berechtigungsobjekten	5	1
X	2	Benutzer anlegen	36	6
X	2	Benutzer ändern	36	6
X	2	Benutzer löschen	36	6
X	2	Benutzer sperren / entsperren / Kennwörter vergeben	36	7
X	1	Benutzern das Profil SAP_ALL zuordnen	28	2
X	2	Benutzern Profile zuordnen	30	6
X	2	Benutzern Rollen zuordnen	29	6
X	1	Aufruf des Reports RSUSR003	102	2
X	1	Benutzer SAP* löschen	36	2
X	1	Ändern des Parameters rec/client	28	11
	1	Ändern des Parameters RECCLIENT im Transportverbund	45	30
X	2	Ändern des Protokollflags für Tabellen	16	2
X	1	Löschen von Tabellenänderungsprotokollen	42	2
X	2	Ändern aller mandantenabhängigen Tabellen	80	2
X	2	Ändern aller Tabellen	54	2
X	2	Lesen aller Tabellen	152	38
X	2	ABAP - Programme anlegen	29	2
X	2	ABAP - Programme ändern	35	2
X	1	Systemänderbarkeit einstellen und ABAPs anlegen oder ändern (ab 7.0)	29	2
X	1	Änderungsbelege löschen	8	2
X	1	Löschen von Tabellenänderungsprotokollen	42	2
X	1	ABAP - Programme debuggen mit Replace	8	2
X	1	ABAP - Quelltexte über RFC installieren und ausführen (ab 7.0)	29	2
X	1	Ausführen aller Funktionsbausteine	35	2
X	1	Versionen löschen	114	
X		(Neue Abfrage ab 01.01.2013)		2
		Summe:	**1528**	**209**

- Das Ergebnis der Prüfung für den Bereich BC umfasst heute 96 kritische Berechtigungen.
- Die Anzahl der Benutzer mit kritischen Berechtigungen konnte weiter reduziert werden.
- Die notwendigen Benutzer mit kritischen Berechtigungen wurden identifiziert und in der Abfrage hinterlegt.
- Das Analyseergebnis liegt heute bei 100 %.
- Änderungen bei der Vergabe der kritischen Berechtigungen werden zeitnah erkannt.

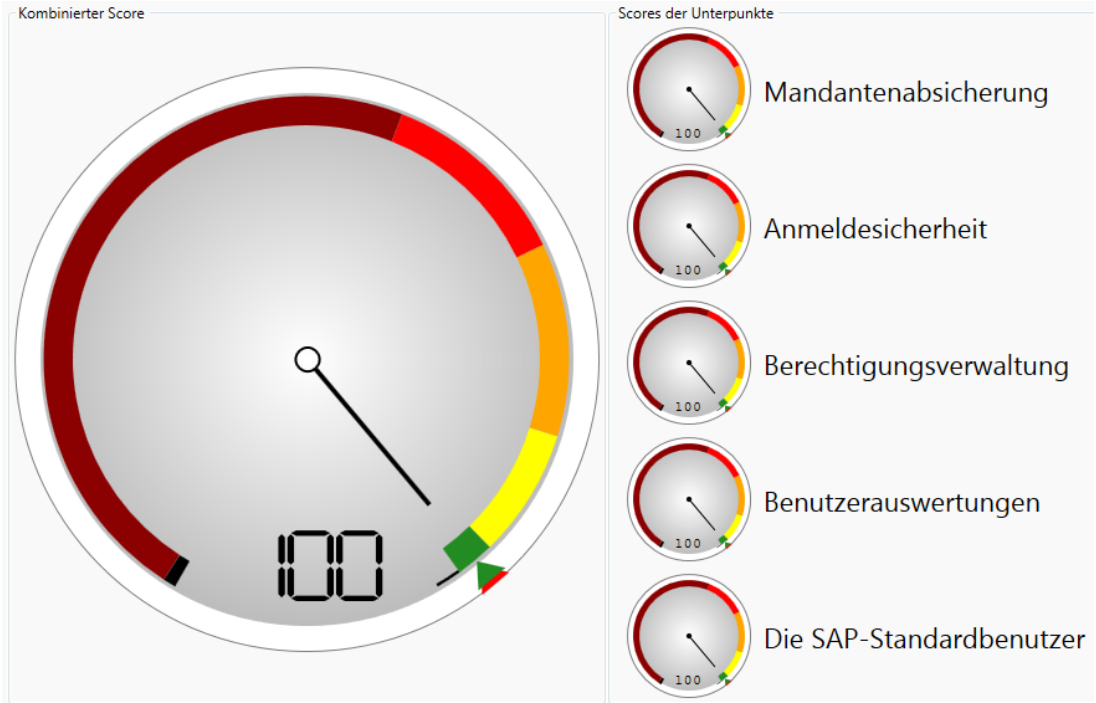


- Mit Hilfe von CheckAud® for SAP® Systems werden diese kritischen Berechtigungen und Einstellung fortlaufend überwacht.
- Zu diesem Zweck wird monatlich ein automatisierter System Scan durchgeführt. Dieser wird mit Hilfe eines definierten Projektbaums ausgewertet.
- Seit der Version CheckAud® for SAP® Systems 2013 nutzen wir die Möglichkeit, autorisierte Benutzer zu definieren und können somit Veränderungen direkt erkennen.



- Die gleiche Vorgehensweise ist auch für die anderen eingesetzten SAP Module möglich.
- Hierbei ist der Arbeitsaufwand jedoch zum Teil wesentlich höher, wenn es sich nicht um Standard SAP Module (Fremd- oder Eigenprogrammierungen) handelt.
- Das gleiche gilt für das Modul PSCD, dessen Funktionalitäten Teile des Moduls FI ergänzt bzw. ersetzt.
- In diesen Fällen müssen die Abfragen zuerst überarbeitet und angepasst werden.
- Die Ergebnisse der Erstprüfung sollten daher mit dem Fachbereichs besprochen werden um „false positive“ Fehler bei den Prüfungsfeststellungen zu vermeiden.

- Die Software CheckAud® for SAP® Systems kann auch für die laufende Überwachung der im SAP® System vergebenen kritischen Berechtigungen genutzt werden und eignet sich deshalb auch für den Einsatz im Rahmen eines Internen Kontrollsystems.



- Der Datenabzug erfolgt getrennt vom Auswertungsmodul und kann z.B. von der Administration durchgeführt werden.

- Die Auswertungen finden getrennt vom SAP®-System statt; daher wird dieses nicht belastet.

- Durch die Prüfung werden 100%ige Ergebnisse erzielt, nicht nur Stichproben basierend auf einzelnen Benutzer- oder Transaktionsauswertungen.

- Die Abfragen werden in einem sog. Projektbaum gespeichert und können jederzeit für weitere Prüfungen verwendet und angepasst werden.

STADT FRANKFURT AM MAIN

- FollowUp Prüfungen sind durch die Vergleichsmöglichkeit ohne großen Mehraufwand möglich
- Es können komplexe Berechtigungsanalysen erstellt werden und wiederholt abgefragt werden
- Zeitersparnis bei der SAP Berechtigungsprüfung
- Sehr hohe Akzeptanz der Prüfungsfeststellungen im geprüften Bereich
- Regelmäßige Versionsaktualisierungen
- Unterstützung im Reporting und IKS-Prozessen
- Einsatz im Rahmen von SAP-Projekten
- Reduzierung des Aufwandes bei der Pflege von SAP-Berechtigungen
- Einsatz durch die Fachabteilung oder durch die Administration möglich
- Einsatz bei wiederkehrenden regelmäßigen Audits im Rahmen des Jahresabschlusses

Vielen Dank für Ihre Aufmerksamkeit!

Fragen ???

Beispiele für Änderungen in SAP S/4HANA

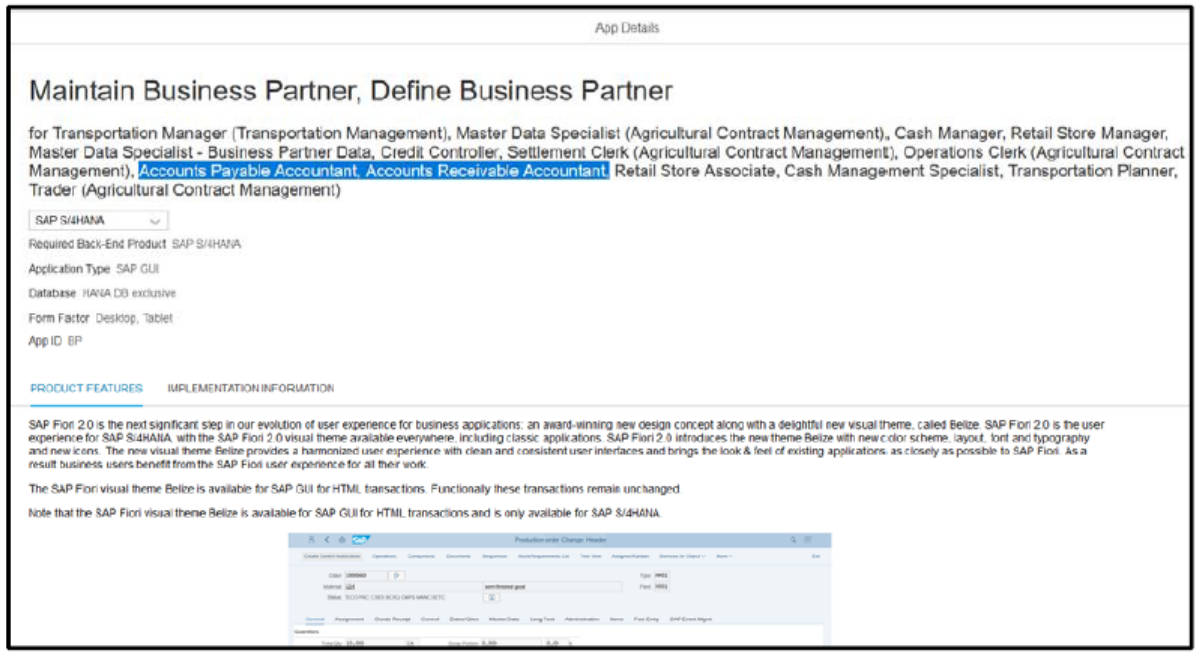
- Stammdaten Debitoren / Kreditoren
  - In SAP ERP werden Kreditoren- und Debitorenstammdaten mit den FK- bzw. FD-Transaktionen gepflegt. In anderen Modulen werden Kreditoren und Debitoren über Geschäftspartner gepflegt.
  - In S/4HANA werden Kreditoren und Debitoren ausschließlich als Geschäftspartner angelegt:
    - Kreditoren: FLVN01
    - Debitoren: FLCU01
  - Folgende Transaktionen sind dadurch in S/4HANA obsolet:

Transaction not available in SAP S/4HANA on-premise edition	FD01, FD02, FD03, FD06, FD0 FK01, FK02, FK03, FK06 MAP1, MAP2, MAP3 MK01, MK02, MK03, MK06, MK12, MK18, MK19, V-03, V-04, V-05, V-06, V-07, V-08, V-09, V-11, V+21, V+22, V+23 VAP1, VAP2, VAP3 VD01, VD02, VD03, VD06 XD01, XD02, XD03, XD06, XD07 XK01, XK02, XK03, XK06, XK07

Beispiele für Änderungen in SAP S/4HANA

- Stammdaten Debitoren / Kreditoren
  - Beim Aufruf der Transaktion FK01 wird zur Transaktion BP verzweigt

  - Alternativ: SAP Legacy-App BP



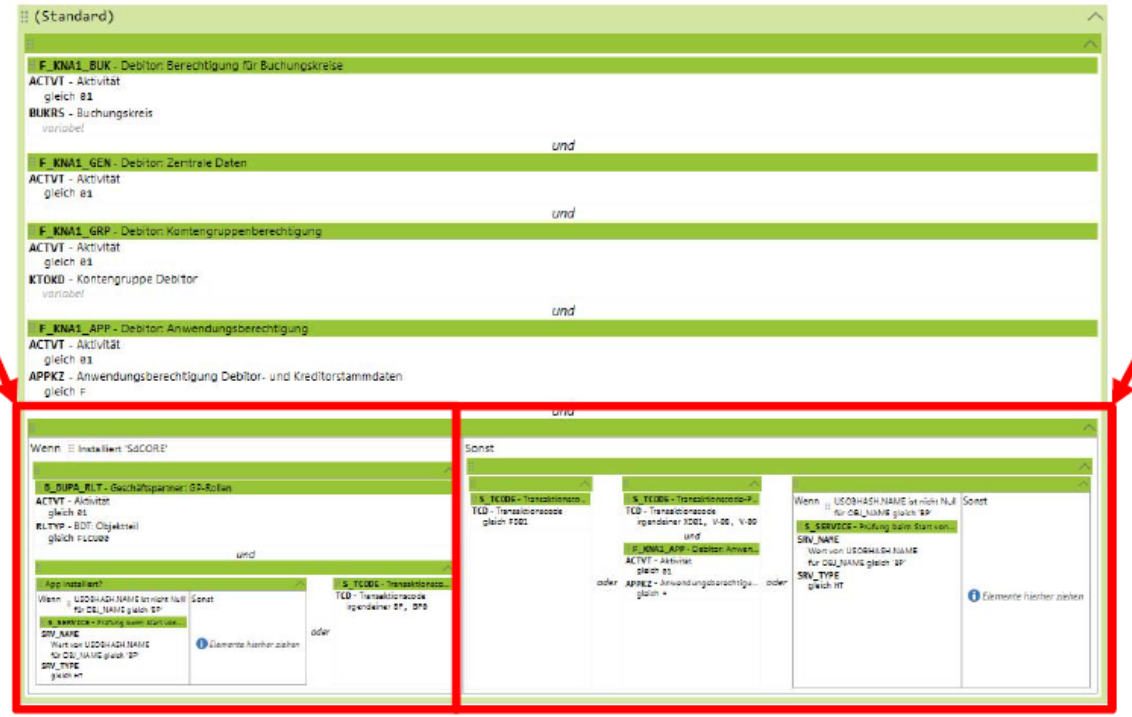
Prüfung von S/4HANA-Berechtigungen mit CheckAud for SAP-Systems

Durch die Release-unabhängigkeit der Abfragen kann auch der Umstieg auf S/4HANA ohne größere Änderungen an den Analyseprojekten erfolgen. Die „**Simplification List for SAP S/4HANA**“ ist in den CheckAud-Abfragen integriert.

Abfrage „*Debitor anlegen (Zentral und Buchungskreis)*“:

In SAP S/4HANA

In SAP ERP

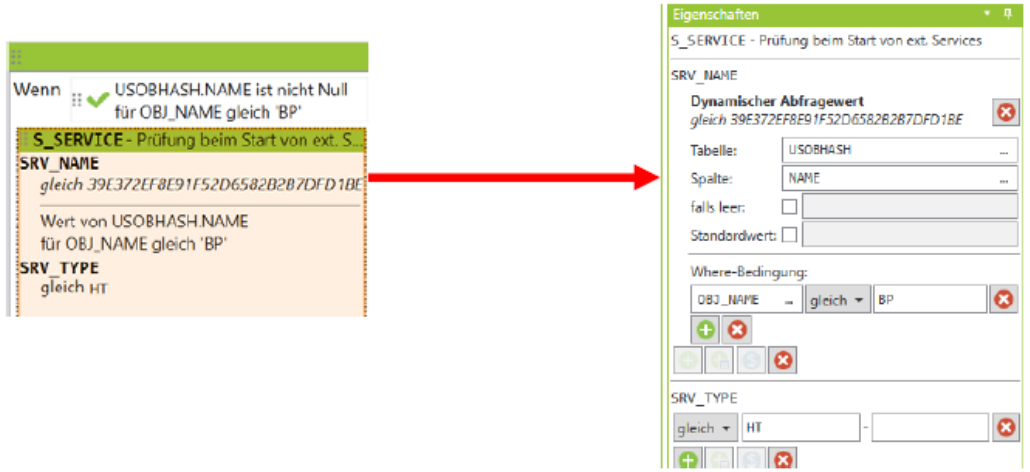


Prüfung von S/4HANA-Berechtigungen mit CheckAud for SAP-Systems

Die App-Berechtigungen werden folgendermaßen abgefragt:

1. Prüfung, ob App installiert ist:

2. Ermittlung des Hash-Wertes für die S_SERVICE-Berechtigung:



Stadt Frankfurt am Main
- Der Magistrat -
Revisionsamt

Ulrich Zimmermann
Gutleutstraße 26
60329 Frankfurt am Main

Telefon: +49 69 212 3 48 78
Telefax: +49 69 212 3 07 15

ulrich.zimmermann@stadt-frankfurt.de

Stadt Frankfurt am Main
- Der Magistrat -
Revisionsamt

Roland Zunke
Gutleutstraße 26
60329 Frankfurt am Main

Telefon: +49 69 212 3 65 41
Telefax: +49 69 212 3 07 15

roland.zunke@stadt-frankfurt.de

Informationen zur Prüfsoftware finden Sie unter „www.checkaud.de“