



## 12. Gipfeltreffen der SAP-Community

# Finanzprozesse mit SAP SAP-Security und Compliance Personalprozesse mit SAP



[it-onlinekonferenz.de](https://www.it-onlinekonferenz.de) | 09.-11.05.23 | #itok23



# Von Can-Do zu Did-Do-Analysen im SAP-System



**Ingo Wihl**  
(IBS Schreiber GmbH)



**Johannes Schwarzenberger**  
(IBS Schreiber GmbH)



**Helge Sanden**  
(IT-Onlinemagazin)

# Unser Portfolio

Wir sind seit über 40 Jahren führender Knowhow-Lieferant für SAP-Security im D-A-CH Markt

In den folgenden Bereichen können wir Sie unterstützen...

## Audit



### SAP Berechtigungen & Compliance

- Basis- und Modulberechtigungen
- Penetrationstest auf Geschäftsprozesse
- S/4HANA® Berechtigungsmigration
- S/4HANA® Datenmigration
- Data Analytics / Did-Do-Analysen

### SAP Security

- Basis- und Systemsicherheit
  - Schnittstellensicherheit
  - HANA DB Sicherheit
- Systemlandschaft & Produktivsystem

## GRC Software / Services



### CheckAud®

Externes Werkzeug zur Prüfung der Berechtigungsvergabe

### Easy Content Solution

Regelwerke auf Knopfdruck für SAP GRC/ IDM Lösungen

## Akademie



- SAP Security Seminare / Webinare
- IBS Security Convention – das SAP Security Event in Hamburg

### Zertifizierung

Certified Auditor® for SAP Applications (CASA)



# Kategorisierung von Kontrollen in SAP

Art der Kontrolle	Eigenschaft	Beispiel
Berechtigungsvergabe	Präventiv	Verhindern von kritischen Berechtigungskombinationen (Bestellung, Wareneingang, Logistische Rechnungsprüfung)
Applikations- und Konfigurationskontrollen	Präventiv	Warenausgang kann nur gebucht werden, wenn ein Kundenauftrag vorliegt.  Bei der Änderung kritischer Felder im Kreditorenstamm (Bankverbindung) wird dieser gesperrt und ein zweites und anderes Benutzerkonto muss diesen freigeben.
Manuelle Kontrollen	Präventiv / Detektiv	Die Einhaltung der administrativen Bestimmungen bezüglich der CpD-Lieferanten.
Halbautomatisierte Analysen	Detektiv	Externe Datenanalysen; Auswertung von Protokollen; Auswertung der Datenbestände (z.B. direkte manuelle Buchungen im Hauptbuch)
Automatisierte Überwachung	Detektiv	Toolgestützte Analysen

# Can Do / Did-Do-Analysen

Level	Beschreibung	Erläuterung
1	Can-Do	Die Can-Do-Analyse konzentriert sich auf die vergebenen Berechtigungen. Sie ist eine Momentaufnahme der aktuellen Situation und gibt Aufschluss darüber, über welche Rechte die Benutzer verfügen.
2	Started Transactions	Auf der Grundlage des Transaktionscodes gibt die Protokollierung dieser Analyse Aufschluss über die von allen Benutzern initiierten Transaktionscodes. <ul style="list-style-type: none"><li>• Gestartete Transaktionscodes für jeden Benutzer</li><li>• Oftmals ist eine Protokollierung von höchstens ca. drei Monaten verfügbar</li><li>• Anonymisierte / nicht anonymisierte Benutzerstatistik</li></ul>
3	Did-do-High Level (irgendein Vorgang)	Buchung / Änderungen von Dokumenten oder Stammdaten <ul style="list-style-type: none"><li>• Mögliche Verletzung der Funktionstrennungskonflikte</li><li>• Auf der Grundlage von Datenanalysen</li><li>• Kann falsch positive Ergebnisse melden</li></ul>
4	Did-do-Detail (gleicher Vorgang)	Buchung/Änderung desselben Dokuments und/oder Nutzung geänderter Stammdaten <ul style="list-style-type: none"><li>• Tatsächliche Verletzung der Funktionstrennungskonflikte</li><li>• Auf der Grundlage von Datenanalysen</li></ul>

# Unterschiede zwischen Can-Do- und Did-Do-Analysen

	Can-Do-Analyse	Did-Do-Analyse
Ziel	Verhindern von kritischen Aktionen (präventiv)	Aufdecken von kritischen Aktionen (detektiv)
Zeit	Zeitpunkt	Zeitraum
Frequenz	Mindestens jährlich	Mindestens quartalsweise
Folgetätigkeit	Veränderung von Berechtigungen Mitigieren der Risiken (z.B. Did-Do-Analysen)	Impact-Analyse der kritischen Aktivitäten Veränderung von Berechtigungen

# Did-Do High-Level-Analyse

## Auswertung der Bestellungen pro User

**Allgemeine Tabellenanzeige**

Hintergrund Anzahl Einträge Alle Eingaben Hinweis 1636416

Datenbankverbindung:

Tabelle: **EKKO**

Texttabelle:

Anzeigevariante:

Maximale Trefferzahl:

Outer-Join-Definition:

Einkaufsbelegkopf:  Ohne Texte  Einträge pflegen

Selektionskriterien

Feldname	O..	Von-Wert	Bis-Wert	Mehr	Gruppe	Ausgabe	Summieren	Gruppieren
Mandant								
Einkaufsbeleg						<input checked="" type="checkbox"/>		<input type="checkbox"/>
Buchungskreis						<input checked="" type="checkbox"/>		<input type="checkbox"/>
Belegtyp						<input checked="" type="checkbox"/>		<input type="checkbox"/>
Belegart						<input checked="" type="checkbox"/>		<input type="checkbox"/>
Steuerung						<input checked="" type="checkbox"/>		<input type="checkbox"/>
LöschKennz						<input checked="" type="checkbox"/>		<input type="checkbox"/>
Status						<input checked="" type="checkbox"/>		<input type="checkbox"/>
Angelegt am		01.01.2014	31.12.2014			<input checked="" type="checkbox"/>		<input type="checkbox"/>
Angelegt von						<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>

**EKKO: Anzeige der gefundenen E**

Zu durchsuchende Tabelle: EKKO

Anzahl Treffer: 57

Laufzeit: 0

ERNAM	LINE_INDEX
ANDERSON	1
BLACKM	21
BLYTH	2
C5157655	156
C5162783	11
C5189771	1
C5202071	33
C5202861	15
C5202937	2
C5207262	4
CPM-PM	74
CPMECO	8
CRMREMOTE	1
D054773	3
DEVELOPER	2
EMPLOYEE	1
EWMCLKU	2
<b>GRAUENHORST</b>	<b>19</b>
HIETT	44

# Did-Do High-Level-Analyse

## Auswertung der angelegten Wareneingänge pro User

**Allgemeine Tabellenanzeige**

Hintergrund Anzahl Einträge Alle Eingaben Hinweis 1636416

Datenbankverbindung  Outer-Join-Definition

Tabelle  Belegkopf Materialbeleg

Texttabelle

Anzeigevariante

Maximale Trefferzahl

Ohne Texte

Einträge pflegen

Selektionskriterien

Feldname	O..	Von-Wert	Bis-Wert	Mehr	Gruppe	Ausgabe	Summieren	Gruppieren
Mandant								
Materialbeleg						<input checked="" type="checkbox"/>		<input type="checkbox"/>
MatBelegjahr						<input checked="" type="checkbox"/>		<input type="checkbox"/>
Vorgangsart						<input checked="" type="checkbox"/>		<input type="checkbox"/>
Belegart		WE				<input checked="" type="checkbox"/>		<input type="checkbox"/>
BelegartUmbew						<input checked="" type="checkbox"/>		<input type="checkbox"/>
Belegdatum						<input checked="" type="checkbox"/>		<input type="checkbox"/>
Buchungsdatum						<input checked="" type="checkbox"/>		<input type="checkbox"/>
Erfasst am		01.01.2014	31.12.2014			<input checked="" type="checkbox"/>		<input type="checkbox"/>
Erfäbt um						<input checked="" type="checkbox"/>		<input type="checkbox"/>
Geändert am						<input checked="" type="checkbox"/>		<input type="checkbox"/>
Benutzername						<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>

Zu durchsuchende Tabelle	MKPF
Anzahl Treffer	28
Laufzeit	0

USNAM	LINE_INDEX
ANDERSON	2
C5177271	9
C5188816	2
C5202071	4
C5202861	3
C5202937	2
C5213966	4
CPM-PM	197
CPMECO	21
D054773	1
GRAUENHORST	14
T001524	4

# Did-Do High-Level-Analyse

Auswertung der angelegten Rechnungen pro User

**Allgemeine Tabellenanzeige**

Hintergrund Anzahl Einträge Alle Eingaben Hinweis 1636416

Datenbankverbindung  Outer-Join-Definition

Tabelle  Belegkopf Eingangsrechnung

Texttabelle

Anzeigevariante

Maximale Trefferzahl

Ohne Texte

Einträge pflegen

**Selektionskriterien**

Feldname	O..	Von-Wert	Bis-Wert	Mehr	Gruppe	Ausgabe	Summieren	Gruppieren
Mandant								
RechnBelegnum.						<input checked="" type="checkbox"/>		<input type="checkbox"/>
Geschäftsjahr						<input checked="" type="checkbox"/>		<input type="checkbox"/>
Belegart						<input checked="" type="checkbox"/>		<input type="checkbox"/>
Belegdatum						<input checked="" type="checkbox"/>		<input type="checkbox"/>
Buchungsdatum						<input checked="" type="checkbox"/>		<input type="checkbox"/>
Benutzername						<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>
Transaktionscode						<input checked="" type="checkbox"/>		<input type="checkbox"/>
Erfasst am		01.01.2014	31.12.2014			<input checked="" type="checkbox"/>		<input type="checkbox"/>

**RBKP: Anzeige der gefunde**

Zu durchsuchende Tabelle	RBKP
Anzahl Treffer	13
Laufzeit	00:

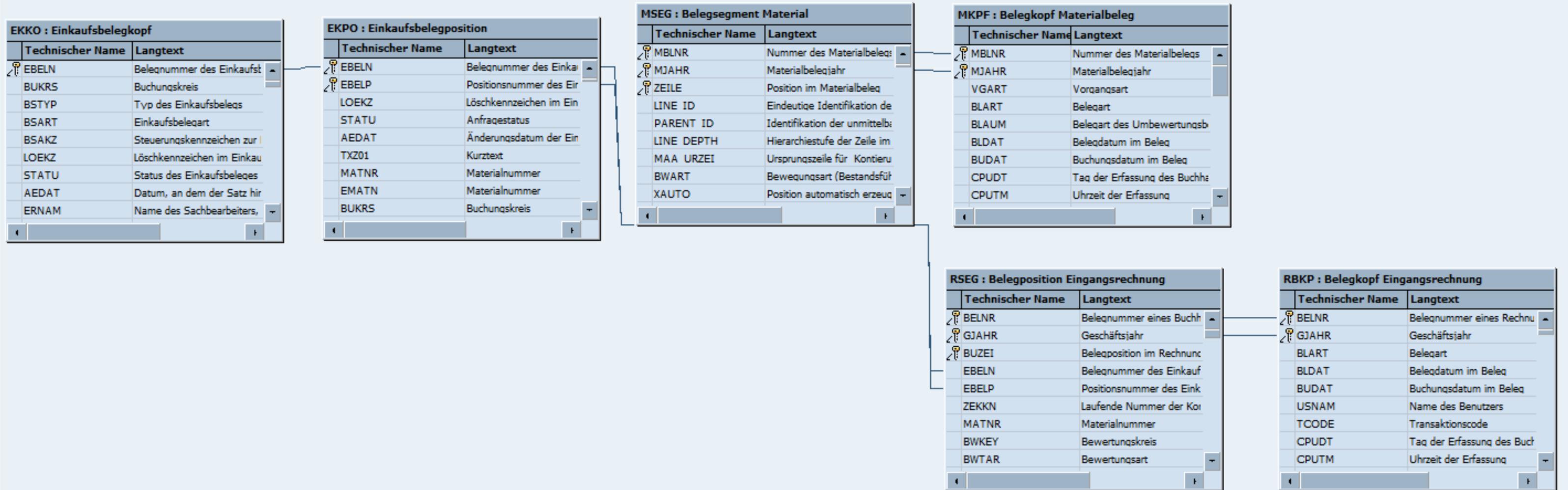
USNAM	LINE_INDEX
C5192081	1
C5202861	2
C5202937	6
CPM-PM	2
CPMECO	3
<b>GRAUENHORST</b>	<b>14</b>
I004952	11
I305033	1
I807095	1
I810890	7
I814325	5
PSUSER	1
PURCHASER	4

# Did-Do High-Level-Analyse

Zusammenführung der Teilergebnisse

User	Bestellu	Wareneinga	Rechnu	Alle Vorgänge
CPM-PM	74	197	2	WAHR
GRAUENHORST	19	14	14	WAHR
C5202861	15	3	2	WAHR
I810890	14	7	7	WAHR
PURCHASER	14	3	4	WAHR
I004952	11	11	11	WAHR
I814325	11	7	5	WAHR
CPMECO	8	21	3	WAHR
I807095	4	2	1	WAHR
I305033	3	2	1	WAHR
C5202937	2	2	6	WAHR
PSUSER	2	1	1	WAHR
C5177271		9		FALSCH
USERADMIN		23		FALSCH
C5192081			1	FALSCH
MRPUSER	264			FALSCH
C5157655	156			FALSCH
HUETT	44			FALSCH
C5202071	33	4		FALSCH

# Did-Do-**Detail**analyse – Einkaufsprozess



# Did-Do-**Detail**analyse – Einkaufsprozess - Ergebnis

PTP Prozess											
BuKr	EinkBeleg	Angel.von	Angel.am	MatBeleg	MJahr	ErfDatum	Name des Benutzers	Belegnr	Jahr	Name des Benutzers	ErfDatum
2222	4500017855	I004952	31.01.2014	5000000562	2014	31.01.2014	I004952	5105609214	2014	I004952	31.01.2014
2222	4500017862	I004952	08.02.2014	5000000581	2014	08.02.2014	I004952	5105609223	2014	I004952	08.02.2014
3000	4500017870	GRAUENHORST	14.02.2014	5000000590	2014	14.02.2014	GRAUENHORST	5105609232	2014	GRAUENHORST	14.02.2014
3000	4500017890	GRAUENHORST	18.02.2014	5000000616	2014	18.02.2014	GRAUENHORST	5105609242	2014	GRAUENHORST	18.02.2014
3000	4500018079	PURCHASER	20.03.2014	5000000650	2014	20.03.2014	PURCHASER	5105609252	2014	PURCHASER	20.03.2014
3000	4500018122	I810890	02.05.2014	5000000712	2014	02.05.2014	I810890	5105609295	2014	I810890	02.05.2014
1000	4500018465	C5202937	08.07.2014	5000000810	2014	08.07.2014	C5202937	5105609322	2014	C5202937	08.07.2014
1000	4500018465	C5202937	08.07.2014	5000000810	2014	08.07.2014	C5202937	5105609323	2014	C5202937	08.07.2014
1000	4500018465	C5202937	08.07.2014	5000000810	2014	08.07.2014	C5202937	5105609324	2014	C5202937	08.07.2014
2222	4500018471	I004952	14.07.2014	5000000822	2014	14.07.2014	I004952	5105609334	2014	I004952	14.07.2014
2222	4500018471	I004952	14.07.2014	5000000822	2014	14.07.2014	I004952	5105609335	2014	I004952	14.07.2014
2222	4500018471	I004952	14.07.2014	5000000823	2014	14.07.2014	I004952	5105609334	2014	I004952	14.07.2014
2222	4500018471	I004952	14.07.2014	5000000823	2014	14.07.2014	I004952	5105609335	2014	I004952	14.07.2014
3000	4500018594	GRAUENHORST	10.10.2014	5000000950	2014	10.10.2014	GRAUENHORST	1000000030	2013	GRAUENHORST	10.10.2014
3000	4500018594	GRAUENHORST	10.10.2014	5000000950	2014	10.10.2014	GRAUENHORST	1000000030	2013	GRAUENHORST	10.10.2014
3000	4500018593	GRAUENHORST	10.10.2014	5000000951	2014	10.10.2014	GRAUENHORST	1000000031	2013	GRAUENHORST	10.10.2014
3000	4500018593	GRAUENHORST	10.10.2014	5000000951	2014	10.10.2014	GRAUENHORST	1000000031	2013	GRAUENHORST	10.10.2014
3000	4500018592	GRAUENHORST	10.10.2014	5000000952	2014	10.10.2014	GRAUENHORST	1000000032	2013	GRAUENHORST	10.10.2014
3000	4500018591	GRAUENHORST	10.10.2014	5000000953	2014	10.10.2014	GRAUENHORST	1000000033	2013	GRAUENHORST	10.10.2014
3000	4500018590	GRAUENHORST	10.10.2014	5000000954	2014	10.10.2014	GRAUENHORST	1000000034	2013	GRAUENHORST	10.10.2014

# IBS Security Convention 2023

Das SAP-Security-Event in Hamburg

Erleben Sie an zwei Tagen hochkarätige Referenten/innen aus der SAP-Security-Szene zu Themen wie:

- ✓ Governance, Risk und Compliance
- 🗄️ SAP HANA® Datenbanksicherheit
- 🚒 SAP-Hacking
- 🧱 Funktionstrennungskonflikte (SoDs)
- ☁️ Cloud-Security und Berechtigungen

Für die zwei Veranstaltungstage erhalten Sie 10 CPEs.

Gemeinsam mit unseren Partnern vor Ort **Convista Consulting, One Identity, Protiviti & Nashcon** freuen wir uns auf Ihre Teilnahme.

Zur  
Agenda



29.06. & 30.06.2023

smart.  
safe.  
compliant.

Fragen?

