



Effiziente und transparente Kontrollen in SAP

Dkfm. Ralph Grunge

Ralph Grunge Consulting GesmbH

Otto Erbert

Siemens IT Solutions and Services



Agenda

Effiziente und transparente Kontrollen in SAP:

- 1 Anforderungen an das Interne Kontrollsystem in SAP im Bereich Public Sector
- 2 Wirksame Umsetzung in SAP f. das Interne Kontrollsystem
 - IKS SAP Berechtigungsexplorer
 - Fraud Explorer
- 3 Praxisrelevante Umsetzung





Internes Kontrollsystem im Public Sector

1

Das Interne Kontrollsystem (IKS) ist ein Managementinstrument, welches die Unternehmensziele sicherstellen soll und in den Bereichen Prozesse, Informationen, Vermögensschutz und Compliance eingesetzt wird. Es umfasst hierbei alle dafür von der Geschäftsleitung angeordneten organisatorischen Methoden und Maßnahmen.

2

Anforderung auch für den Public Sector Bereich, die Funktionsfähigkeit, Wirksamkeit, Wirtschaftlichkeit und Angemessenheit des Internen Kontrollsystems nachweisen zu können.



Bisherige Erfahrung zum IKS im Bereich Public Sector

SIEMENS

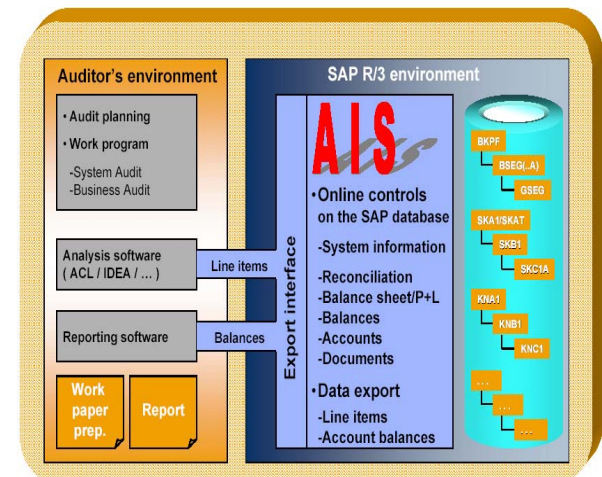
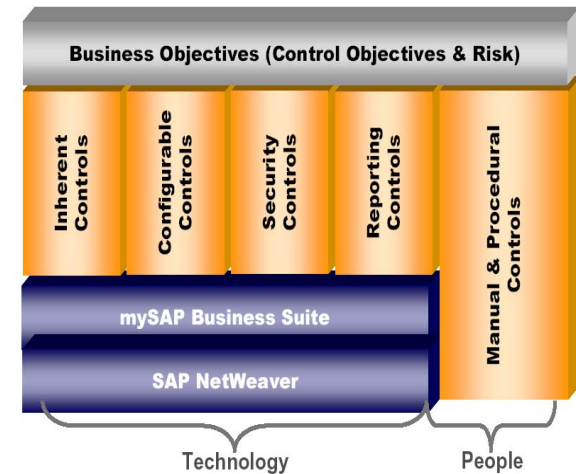
- Es zeigt sich, dass bei den gegenwärtigen Ausprägungen Kontrollen im Regelfall stark informell durchgeführt werden und die Nachweise sehr zeitaufwändig über manuelle Vorgehensweisen erbracht werden.
- In Folge ergibt sich ein hoher Arbeitsaufwand bei gleichzeitig stark wachsender Erwartungshaltung, bspw. Rechnungshofprüfer an Durchführung und Dokumentation des IKS.
- Hohe Ausstrahlungswirkung der gesetzlichen Anforderungen aus Privatwirtschaft





Automatische Kontrollen im SAP-Standard!

- SAP verfügt im Standard über rund **500 Kontrollen** des Financial Reporting.
- Im Standard heißt insbesondere auch, dass diese **kostenfrei**, ohne zusätzliche Lizenzgebühren genutzt werden können!
- Viele dieser SAP Standardkontrollen können im Regelfall sehr rasch im Customizing aktiviert und genutzt werden!
- *Das Monitoring über diese Kontrollen kann ebenfalls in hohem Grade **automatisiert** werden!*





Effizientes Reporting über die IKS Konformität der SAP Berechtigungen

SIEMENS

Wirksamer Einbezug der SAP Berechtigungen

Schnelles Reporting über die sensiblen Berechtigungen (Beispiel elektronisches Radieren, Benutzerpflege, Kreditorenstammdatenpflege...)

Schnelles Reporting auf Funktionstrennungskonflikte

Verwendung von Best Practice Regelsets über alle relevanten SAP Prozesse und den SAP Basis Berechtigungen



Live Demo Vorgehensweise SAP Berechtigungen

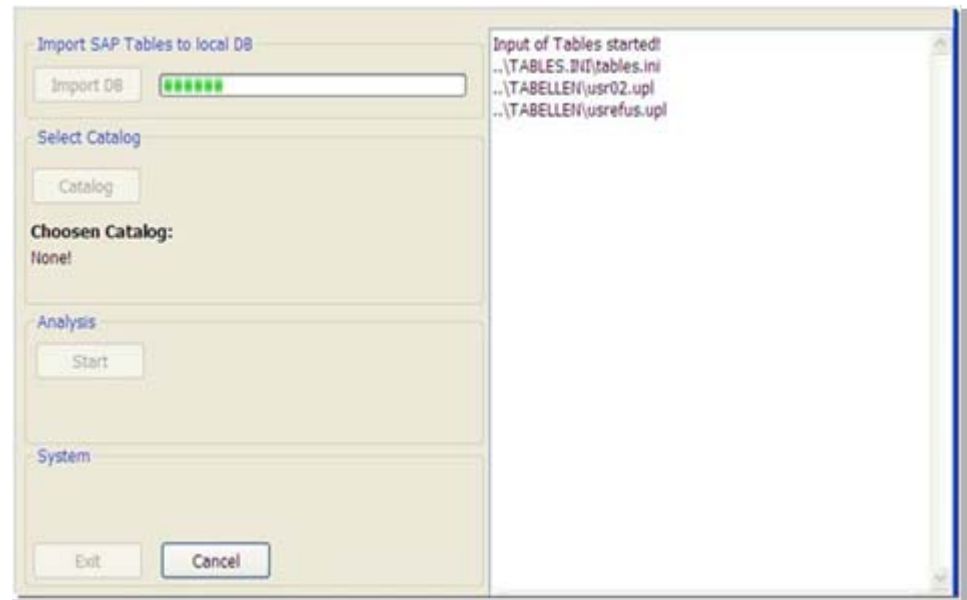
	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1		BIT_DS9_5_2_Customizing_SM30_Tabellen	BIT_DS5_7_1_SM35_Batchinput_Loschberech	BIT_DS5_9_SNUM_Nummernkreispflegeberec	BIT_DS5_8_2_SU02_Anlegen_Aktivieren_Prof	BIT_DS5_9_SNRO_Nummernkreispflegeberec	BIT_DS9_1_1_Pflegeberechtigungen_Tabellen	BIT_DS5_6_SM49_Betriebssystemkommandos	BIT_DS5_8_4_SU01_Manuelles_Anlegen_von_B	BIT_DS5_8_5_SU01_Manuelles_Andern_von_B	BIT_DS5_5_RFCberechtigungen	BIT_DS9_5_3_Customizing_SM31_Tabellen	BIT_DS5_9_Nummernkreispflegeberechtigung	BIT_DS5_8_3_PFCG_Anlegen_Aktivieren_Rolk
2	Total	46	72	31	25	39	71	34	25	25	35	42	216	29
3	DEMO1	X	X	X	X	X	X	X	X	X	X	X	X	X
4	DEMO2	X	X	X	X	X	X	X	X	X	X	X	X	X
5	DEMO3	X	X	X	X	X	X	X	X	X	X	X	X	X
6	DEMO6	X	X	X	X	X	X	X	X	X	X	X	X	X
7	DEMO22	X	X	X	X	X	X	X	X	X	X	X	X	X
8	DEMO41	X	X	X	X	X	X	X	X	X	X	X	X	X
9	DEMO52	X	X	X	X	X	X	X	X	X	X	X	X	X
10	DEMO67	X	X	X	X	X	X	X	X	X	X	X	X	X
11	DEMO82	X	X	X	X	X	X	X	X	X	X	X	X	X



Verfügbare Standard Regelsets zzgl. den Branchenlösungen IS-P

SIEMENS

- Einkauf/Vertrieb
- Financial Reporting/
Anlagenbuchhaltung
- Human Resources
- Materialwirtschaft
- SAP Basis
- CoBIT/COSO
- Fraud Prevention
- IS-H/i.s.h.med
- IS-P/PS-CD
-





Erweiterung um Prozesskontrollen (Fraud-detection & prevention)



Effizientes Reporting der SAP Prozesskontrollen

Vorgehensweise bei Prozesskontrollen:

Schnelles Erkennen von aufgetretenen Funktionstrennungskonflikten in den SAP Stamm- und Bewegungsdaten

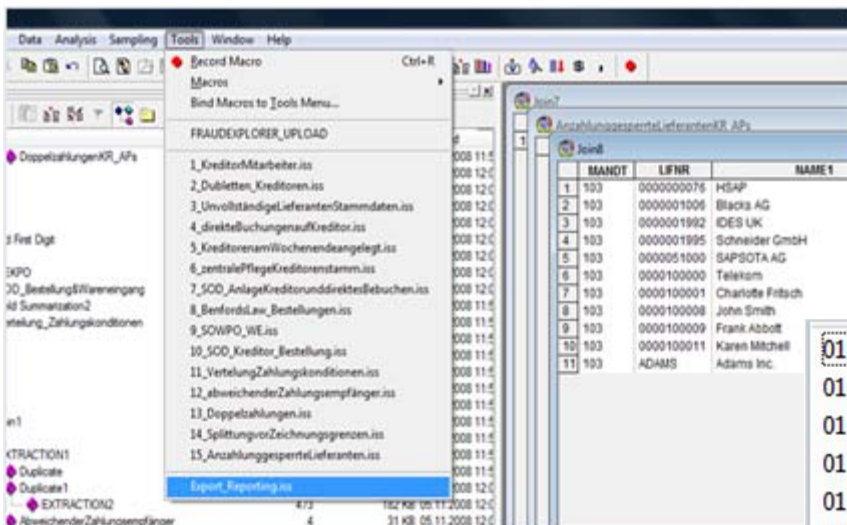
Schnelles Erkennen von möglichen Manipulationen an IKS relevanten Customizingeinstellungen oder Stammdaten

Statistische Analysen (Benford...)

...



Ergebnisdarstellung der automatisierten Verfahrensweise



01.11.2008 ...	1_MitarbeitermiteBankverbindungKre...	XSD-Datei
01.11.2008 ...	2_Dubletten	XML-Dokume
01.11.2008 ...	2_Dubletten.xsd	XSD-Datei
01.11.2008 ...	3_KreditorenohneOrt	XML-Dokume
01.11.2008 ...	3_KreditorenohneOrt.xsd	XSD-Datei
01.11.2008 ...	3_KreditorenohneStraße	XML-Dokume
01.11.2008 ...	3_KreditorenohneStraße.xsd	XSD-Datei
01.11.2008 ...	3_KreditorenohneTelefonnummer	XML-Dokume
01.11.2008 ...	3_KreditorenohneTelefonnummer.xsd	XSD-Datei
01.11.2008 ...	4_DirekteBuchungenKR_AP's	XML-Dokume
01.11.2008 ...	4_DirekteBuchungenKR_AP's.xsd	XSD-Datei
01.11.2008 ...	4_DirekteBuchungenOPS	XML-Dokume
01.11.2008 ...	4_DirekteBuchungenOPS.xsd	XSD-Datei
01.11.2008 ...	5_AnlageamWochende	XML-Dokume
01.11.2008 ...	5_AnlageamWochende.xsd	XSD-Datei





Inhalte der Prozesskontrollen

1

Nachweis über mögliche Funktionstrennungskonflikte

2

Nachweis über anforderungsgerechte Geschäftsprozesse

3

Nachweis der Funktionsfähigkeit der Customizingeinstellungen



**Praxisrelevante
Umsetzung der
IT-unterstützten
Dienstleistungen
für SAP in der
Siemens IT-Revision,
Region CEE**



Siemens IT-Revision für Region CEE

Verantwortliche Durchführung von IT-Prüfungen in:

- 12 Staaten
- ca. 100 Siemens Gesellschaften
- mit ca. 25 IT-Revisoren

In den Hauptgebieten

- SAP
- Informationssicherheit (ISO 2700x)

ca. 100 Revisionsberichte pro Jahr



IT-Audit Programm SAP

- 1 Einführungs- und Prozessprüfungen
- 2 Einbettung ERP-System (Rechnerraum, Workstation, Datenbank, ...)
- 3 GoBS-Prüfungen (Grundsätze ordnungsgemäßer Buchführungs-Systeme) des SAP Systems – mit Anerkennung durch WP-Kanzlei – Ausstellung Prüfpass
- 4 Berechtigungskonzepte
- 5 Fraud-Prüfungen (Detection and Prevention)



Argumente für die Durchführung von IT-gestützten SAP Prüfungen

Klassische Revisionsgründe:

- Compliancegründe
- Ordnungsmäßigkeit
- Datenintegrität
- Datensicherheit
- Zukunftssicherheit
- ...



Argumente für die Durchführung von IT-gestützten SAP Prüfungen

SIEMENS

Wachsender Druck auf Gesellschaften zur **Verkürzung von Abschlusszeiten**

Abhängigkeit der Unternehmenseinheiten **von** der **Informationsverarbeitung wächst**; IT-Themen werden immer komplexer;

Zentrale Kontrollanforderungen wie Sarbanes Oxley Act, Euro Sox (8. EU Richtlinie 2006/43 §41 = IKS Vorgaben), URÄG, ...

Hebelwirkung der IT auf Geschäftsprozesse ist groß; die systematische Erschließung des "Business Value of IT" ermöglicht erhebliche Produktivitätsfortschritte



Erfolge: SAP – Fraud und IKS Prüfungen

- **Kritische Berechtigungen** wurden aus dem operativen System entfernt (SAP_ALL, SAP_NEW, S_DEVELOP, ...)
- **Neues Berechtigungskonzept**, rollenbasiert unter Berücksichtigung von Organisation und Funktion – Sammelrollen-Vergabe vor Ort (soll Rollenakkumulierung verhindern von z.B. Lehrlingen, Trainees, ...)
- Anwenderdokumentation aktualisiert
- **Klare Kontrollprozesse**: Regelungen in den Gesellschaften von z.B. regelmäßigen Kontrollen (Batch-Input Mappen Verarbeitung, Notfallusereinsatz inkl. deren Dokumentation)
- Prüfung auf Einhaltung von **Funktionstrennungen**. In Einzelfällen (kleine organisatorische Einheiten) Kontrollprozesse, z.B. 4-Augen Prinzip außerhalb von SAP



Erfolge: SAP – Fraud und IKS Prüfungen

SIEMENS

- Bereinigung von Lieferanten – Stammdaten (Doppel- oder Mehrfacherfassung), restriktive Rechtevergabe für User mit Lieferantenstammdatenpflege
- Erkennen von **Doppelzahlungen**

Fraud – Prevention: Kontrolleinstellungen in SAP

- 4-Augen Prinzip mit SAP – Transparenz über die Nutzung
- Optimierte Einstellungen im SAP Customizing, wie z.B. Buchungs- und Toleranzgrenzen



Beispiel aus SAP Fraud Bericht

IT08036 Test_SAP Fraud_Bericht.doc - Microsoft Word

Datei Bearbeiten Ansicht Einfügen Format Extras Tabelle Fenster Livelink ? Adgbe PDF Acrobat-Kommentare Frage hier eingeben

status + Dunke Arial 16

1.2 → Lieferantenstammdaten → Datenqualität → Dubletten	11
1.3 → Unvollständige Lieferantenstammdaten	14
1.4 → Auffälligkeiten wie Testkreditoren oder fehlende Namenskonventionen	15
1.5 → Direkte Buchungen durch fehlende Einkaufssichten	15
1.6 → Wurden Kreditoren zu ungewöhnlichen Zeiten angelegt und zeigen diese ungewöhnliche Umsätze	17
1.7 → Änderungen an Kreditorenstammdaten werden korrekt aufgezeichnet und wurden nicht manipuliert	17
1.8 → Manipulationen an Bankverbindungen	18
1.9 → Zentrale Pflege der Kreditorenstammdaten	19
1.10 → Unterschiedliche Kreditoren verfügen über die gleiche Bankverbindung	20

Seite 2 Ab 2 2/75 Bei Ze Sp MAK ÄND ERW ÜB Englisch (Gr)



Beispiel aus SAP Fraud Bericht

IT08036 AT_RG_SAP Fraud_Bericht.doc - Microsoft Word

Datei Bearbeiten Ansicht Einfügen Format Extras Tabelle Fenster Livellink ? Adgbe PDF Acrobat-Kommentare Frage hier eingeben X

Verzeichnis 2 Arial 14

SIEMENS

1.3 -> Unvollständige-Lieferantenstammdaten -> [Flag]

Zielsetzung/Risiko

Es befinden sich nur autorisierte und vollständig gepflegte Lieferantenstammdaten im System.

Unvollständig gepflegte Lieferantenstammdaten, wie fehlende Telefonnummern, fehlende Anschriften, Postfachadressen (anstelle vollständiger Anschriften), erschweren die Nachvollziehbarkeit und können einen Hinweis auf dolose Handlungen darstellen.

SAP-Test/Analysehandlungen

Überprüfung, ob unvollständige Lieferantenstammdaten im System vorliegend sind.

Ergebnis

Es liegen rund 400 Lieferantenstammdaten vor, die lediglich eine Postfachadresse aber keine Straße in den Stammdaten gepflegt haben. Rund 9.000 Stammsätze haben keine Telefonnummer gepflegt. Zudem liegen Stammsätze vor, bei denen keine Einkaufssicht in den Stammdaten gepflegt ist.

Empfehlung/Hinweise

Es sollte intern diskutiert werden, inwieweit die Stammdaten einer Überarbeitung zuzuführen sind (Bereinigung inaktiver Stammsätze, Nachpflege der Stammsatzinformationen).

Seite 12 Ab 2 12/75 Bei Ze Sp MAK ÄND ERW ÜB Deutsch (De)



Beispiel aus SAP IKS Auswertung

Microsoft Excel - IKS_Siemens_Test_anonym_2008.xls

1.03.120 SE16 Replace in debugging DEBUG

	A	R	S	T	U	V	W	X	Y	Z	AA	AB
1	User	1.03.190 Logical operating system commands (UNIX) SF	1.02.070-1 Analyze emergency user concept Delete SAL	1.06.060 Customizing authorizations Templates Change	1.06.070 TMS Administration functions in CTS SE01	3.10.020 VD06 Vendor/customer master records - dele	6.06.000 MIGO_GR Goods movements	1.03.120 SE16 Replace in debugging DEBUG	1.03.190 Logical operating system commands (UNIX) SF	6.06.050 MEL2 Purchase information records Change	3.10.020 XD06 Vendor/customer master records - dele	3.10.030 FSS0 Main. Auth. for general ledger account
2	Total	85	12	74	85	275	286	4	42	74	71	76
2951	2949											
2952	2950											
2953	2951	X		X	X	X	X		X	X	X	X
2954	2952	X		X	X	X	X		X	X	X	X
2955	2953	X		X	X	X	X		X	X	X	X
2956	2954											
2957	2955	X		X	X	X	X		X	X	X	X
2958	2956	X		X	X	X	X		X	X	X	X
2959	2957											
2960	2958	X		X	X	X	X		X	X	X	X
2961	2959	X		X	X	X	X	X	X	X	X	X

ergbeis0

Bereit

NF



Zusammenfassung

- Große Akzeptanz der Untersuchungen bei CFO und CIO (SAP-Verantwortliche)
- Festlegung auf regelmäßige Untersuchungen (kl. Gesellschaften jährlich, gr. Gesellschaften halbjährlich)
- Achtung: Nach Erstuntersuchung möglicherweise erheblicher „Bereinigungs-Aufwand“
- Berücksichtigung von individuellen Zusatzuntersuchungen oder Schwerpunktsetzungen möglich
- Bereits in allen gr. Siemens Gesellschaften in CEE durchgeführt, aber auch in Siemens Gesellschaften in USA und Deutschland
- Aufgrund dieser internen Erfolgs-Story – Durchführung von IT-gestützten Prüfungen auch für externe Partner möglich



Siemens IT-IKS Lösungen für EU und CEE

IT-Compliance auf Basis 8. EU-Richtlinie

SIEMENS IT-audit consulting

SAP IKS

- IKS-Explorer (Prüfung kritischer Berechtigung nach definierten Regelsets)
- Fraud Explorer (140 Analysehandlungen)
- GoB-Überprüfungen (Grundsätze ordnungsgemäßer Buchführung)

Information Security Überprüfungen

- InfoSec Basisprüfungen
- Prüfungen nach ISO 27001 und ISO 27002
- Zertifizierungsvorbereitung

IT Service Management

- Prüfungen nach ISO 20000 (ITIL)
- Zertifizierungsvorbereitung

Siemens hat umfangreiches Expertenwissen für IT-IKS Prüfungen



Kontakt

SIEMENS

Vielen Dank für Ihre Aufmerksamkeit!

Dkfm. Ralph Grunge

Ralph Grunge Consulting GesmbH

Tel: 0699 10 24 29 30

Otto Erbert

Siemens AG Österreich

Tel: 0664 80117 33770