Applikatorische Schnittstellen – nichts verloren unterwegs?

Prüfung und Überwachung automatischer Schnittstellen im Umfeld von ERP
Eine praktische Anleitung

Nathalie Lacambra, lic. oec. HSG, CISA, CIA
Stefan Gröninger, dipl. Wirtschaftsinformatiker (FH)

05. November 2012

Ausgangslage

Hypothese 1	Hypothese 2	Hypothese 3
„Die Prüfung von Schnittstellen zwischen ERPs und Umsystemen wird häufig vernachlässigt.“	„Die Prüfung von Schnittstellen bedingt vor allem vertieftes IT-Knowhow.“	„Stimmt das Total der Ausgangsdaten mit dem Total der Zieldaten überein, so kann nichts schiefgegangen sein“.

Inhalt

1. Bedeutung von Schnittstellen für die Revision
2. Herausforderungen bei der Schnittstellenprüfung
3. Vorgehen
4. Beispiele
5. Zusammenfassung
6. Fragen

1. Bedeutung von Schnittstellen für die Revision

Bedeutung von Schnittstellen für die Revision

Schnittstellen sollen sicherstellen, dass Daten korrekt und vollständig übertragen werden.

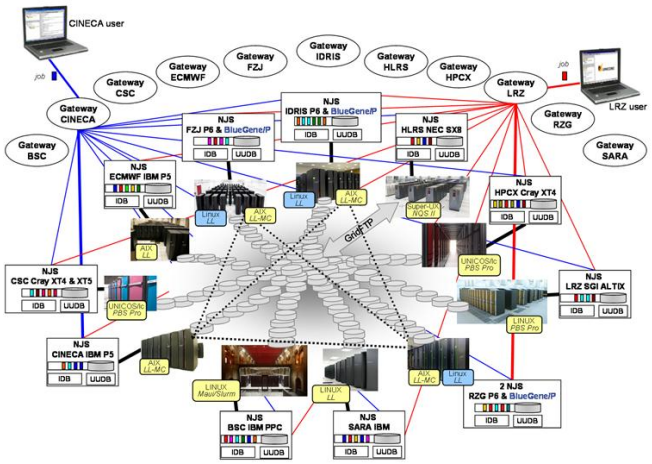
Im Fall von Umsystemen und ERP kommt evt. noch die korrekte Verbuchung hinzu.

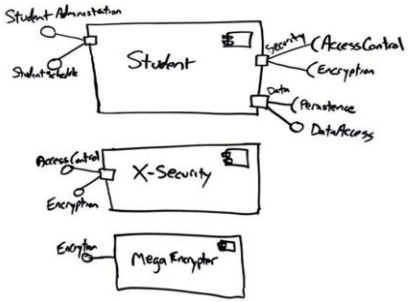
Ansonsten besteht das Risiko, dass u.a. die Richtigkeit und Vollständigkeit von Daten für die finanzielle Berichterstattung beeinträchtigt ist.

2. Herausforderungen bei der Schnittstellenprüfung

Herausforderungen

- Vielfältigkeit der Ausprägung von Schnittstellen ➡ Jede Schnittstelle ist anders
- Technische Komplexität ➡ Oft Black Box
- Komplexität des Datenflusses ➡ Oft Black Box
- Verzahnung von Geschäftsprozessen und IT ➡ Koordination erforderlich
- Unklare Verantwortlichkeiten an Systemgrenzen ➡ Koordination erforderlich
- Unvollständige Dokumentation von Schnittstellen ➡ Zusatzaufwand erforderlich





3. Vorgehen

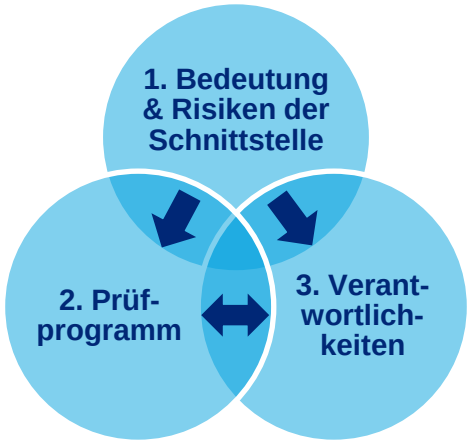
Vorgehen

Zentrale Fragen:

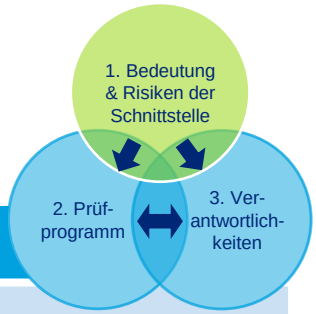
1. Was ist die Bedeutung der applikatorischen Schnittstelle zwischen ERP und Umsystem?
   - ➢ **Verständnis der Bedeutung und Risiken der Schnittstelle**

2. Wie kann die Schnittstelle sinnvoll geprüft werden?
   - ➢ **Ausarbeitung des Prüfprogramms**

3. Welches sind dabei die Aufgaben der Fachrevision und der IT-Revision?
   - ➢ **Abstimmung der Verantwortlichkeiten**

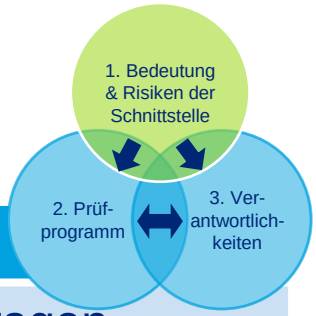


1. Verständnis der Schnittstelle (1/2)



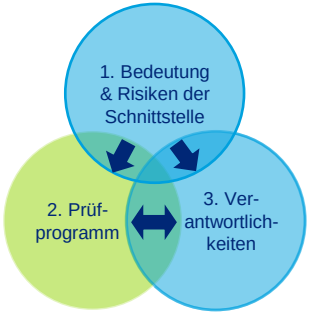
Frage	Mögliche Antworten
Wie ist die Schnittstelle gebaut?	▪ Standard Software ▪ Eigenentwicklung ▪ Kombination ▪ …
Was für Daten werden übertragen?	▪ Stammdaten ▪ Transaktionsdaten ▪ Daten, die für finanzielle Berichterstattung relevant sind ▪ …
Was geschieht innerhalb der Schnittstelle?	▪ Daten unverändert von System A nach System B ▪ Aggregation / Mapping von Daten ▪ Umrechnungen (z.B. von Währungen) ▪ Allokation auf Konten ▪ …

1. Verständnis der Schnittstelle (2/2)



Frage	Mögliche Antworten
Was sind Risiken / Fehlerquellen der Schnittstelle, bzw. was kann die vollständige und korrekte Übertragung gefährden?	▪ Datensätze werden doppelt übertragen ▪ Datensätze werden gar nicht oder nicht vollständig übertragen ▪ Daten werden innerhalb der Schnittstelle ungewollt verändert ▪ …
Sind schon einmal Fehler aufgetreten? Wenn ja, warum?	▪ Falsch programmiertes Mapping von Ausgangs- zu Zielsystem ▪ Systemverfügbarkeit temporär nicht gegeben und deshalb Prozess abgebrochen ▪ Vorhandene Fehlerberichte nicht analysiert ▪ …

2. Ausarbeitung des Prüfprogramms (1/3)

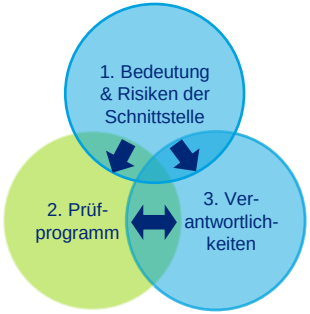


- Prüfzeitpunkt und Prüfart bestimmen
  - Prüfung nach Einführung
  - Einmalige Prüfung im laufenden Betrieb
  - Sich wiederholende Prüfung im laufenden Betrieb (continuous)

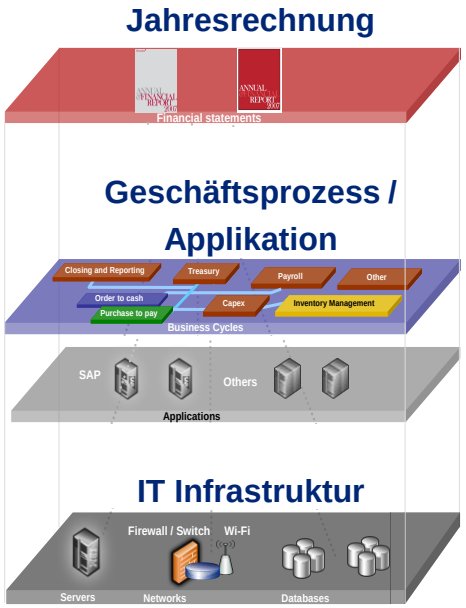
- Ausarbeitung des Prüfprogramms anhand oben gewonnener Informationen

- Identifikation wesentlicher Schlüsselkontrollen - manueller und automatisierter - um alle oben identifizierten Risiken angemessen zu adressieren

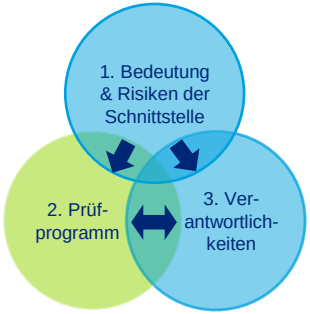
2. Ausarbeitung des Prüfprogramms (2/3)



Bereich	Mögliche Kontrolle
Geschäftsprozess-kontrollen – Manuelle	▪ Abstimmungen (Reconciliations) zwischen Ausgangs- und Zielsystem ▪ …
Geschäftsprozess-kontrollen – Automatisierte	▪ Applikationsregeln für die Bereitstellung der Daten ▪ Einlese-Kontrolle der Zielapplikation ▪ Zugriffsrechte
Geschäftsprozess-kontrollen – Kombinierte	▪ Überprüfung von automatisch erstellten Fehlerberichten ▪ Überprüfung von automatisch erstellten Reports
Generelle IT Kontrollen	▪ Überwachung von Batch-Prozessen ▪ Genehmigungsverfahren bei Konfigurationsänderungen ▪ Zugriffsrechte ▪ Hash-Totals ▪ Testing bei Neuerungen/ Änderungen

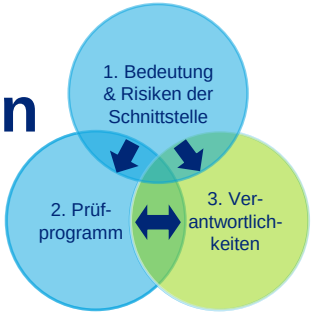


2. Ausarbeitung des Prüfprogramms (3/3)



- In gewissen Fällen bietet es sich an, eine Schnittstelle mit ACL zu prüfen, d.h. die Übertragung der Daten (und mögliche Berechnungen/Daten-Allokationen innerhalb der Schnittstelle) mit ACL nachzubilden und somit die korrekte und vollständige Übertragung zu bestätigen
  - Erhöhter Aufwand
  - Lohnt sich, wenn die Schnittstelle wiederholt geprüft werden soll
  - Erlaubt „Prüfung auf Knopfdruck“

3. Aufgaben der Fachrevision und der IT-Revision



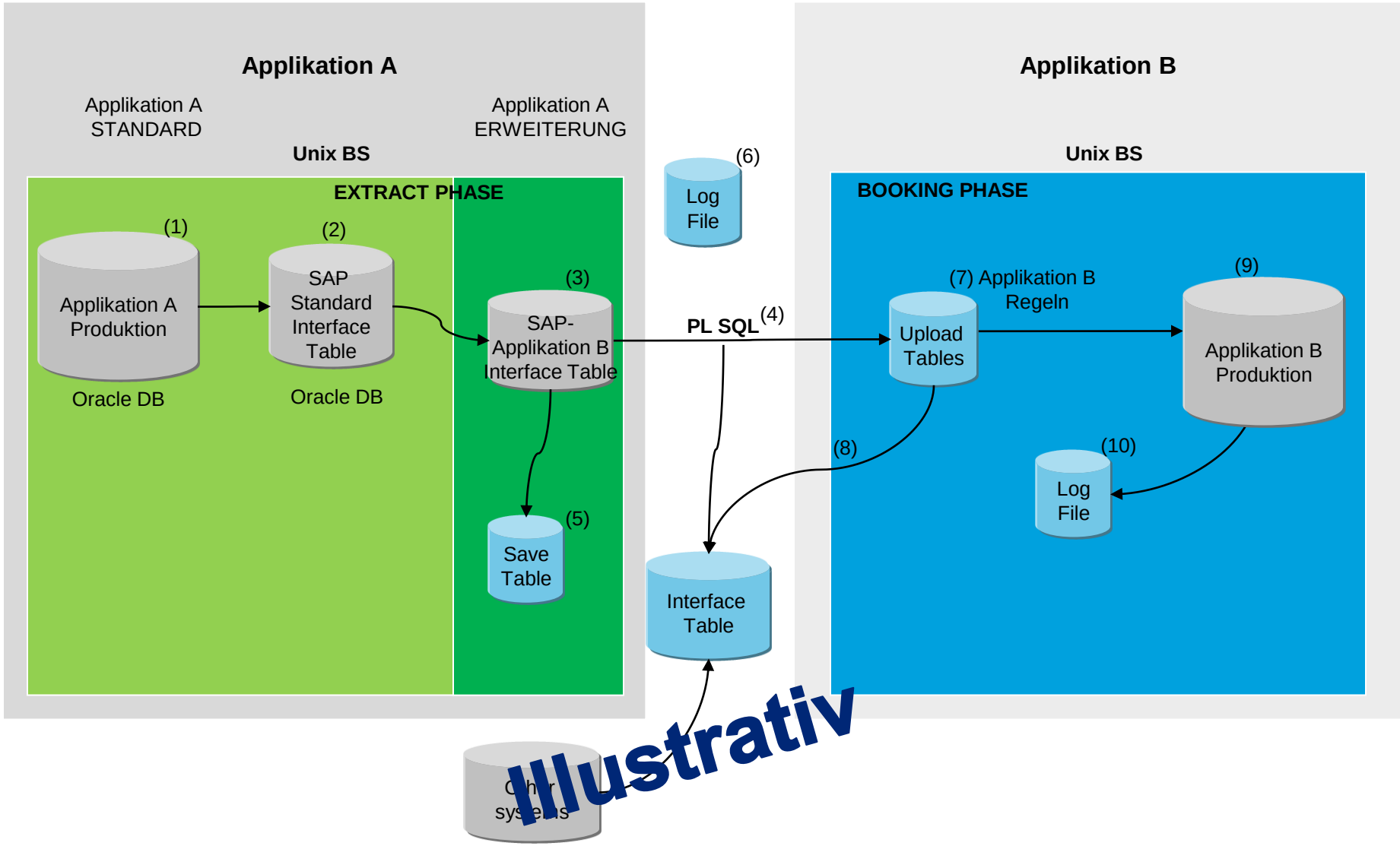
- Idealfall: Gemeinsame Planung und Durchführung

Aufgabe	Verantwortlichkeit
Verständnis der Schnittstelle	➢ Gemeinsam
Beurteilung der Risiken	➢ Gemeinsam
Prüfung manueller Kontrollen im Geschäftsprozess	➢ Fachrevision
Prüfung automatisierter/IT-basierter Kontrollen	➢ IT-Revision
Prüfung kombinierter Kontrollen	➢ Gemeinsam
Prüfung mittels ACL	➢ Gemeinsam
Beurteilung von Prüfresultat und finaler Konklusion	➢ Gemeinsam

4. Beispiele

Beispiel 1: Prüfung von Kontrollen

Verständnis der Schnittstelle (1/2)



Beispiel 1: Prüfung von Kontrollen

Verständnis der Schnittstelle (2/2)

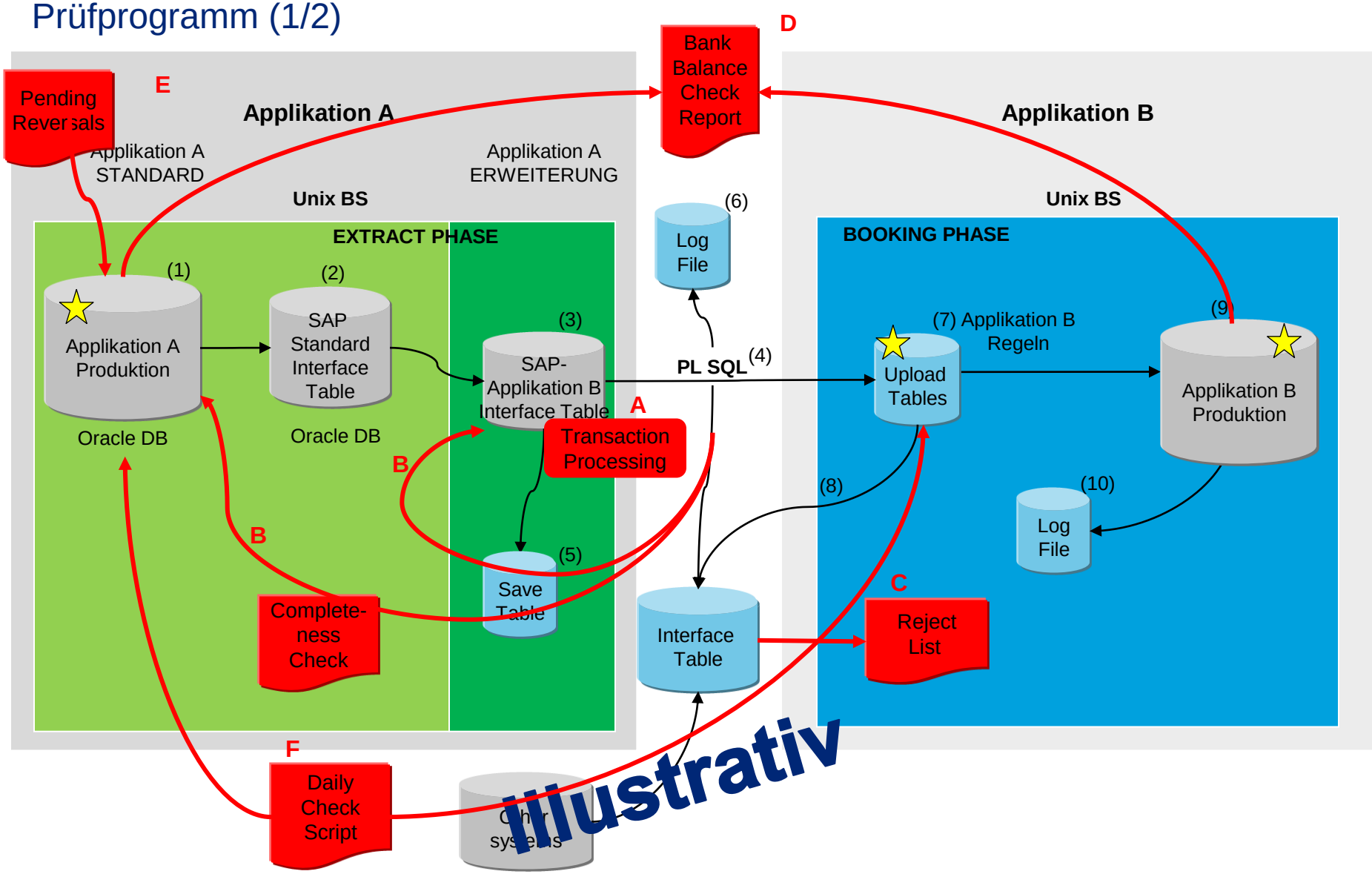
No.	*Short description*
(1)	▪ Application is master for currency rates. ▪ Application processes input from ABC and DEF (payment instructions), and generates money market transactions. ▪ Within Application A, processing is managed by status flags (for details see below "Other Information")

(2)	▪ Main selection criteria: Status flags
	  ▪ Actioned
	  ▪ Not interfaced
	▪ Twice daily batch transfers selected records.
	▪ Only modification to data from (1) to (2): All foreign currencies are converted into US$.
	▪ SAP interface table confirms successful data transfer after the entire transaction has been completed.

(3)	▪ Trigger: As soon as records are extracted from (1) to (2), they are mirrored in real-time from (2) to the SAP-Application b interface table (1:1 copy). ▪ After successful line processing the records are deleted in (2).
(4)	*Major steps during twice daily transfer:* 1. Read access to Application A data, referring to account details (as account details are stored in Application A but not assigned on record level). 2. Mapping of transactions from Application A to Application B account structure ("Kontennummer-Aufschlüsselung") 3. Add versioning number to each deal number 4. Settle Forex bookings 5. Split up Application C collective bookings (1 transaction in Application A generates 2 booking entries in Application B (credit/debit)

Beispiel 1: Prüfung von Kontrollen

Prüfprogramm (1/2)



Beispiel 1: Prüfung von Kontrollen

Prüfprogramm (2/2)

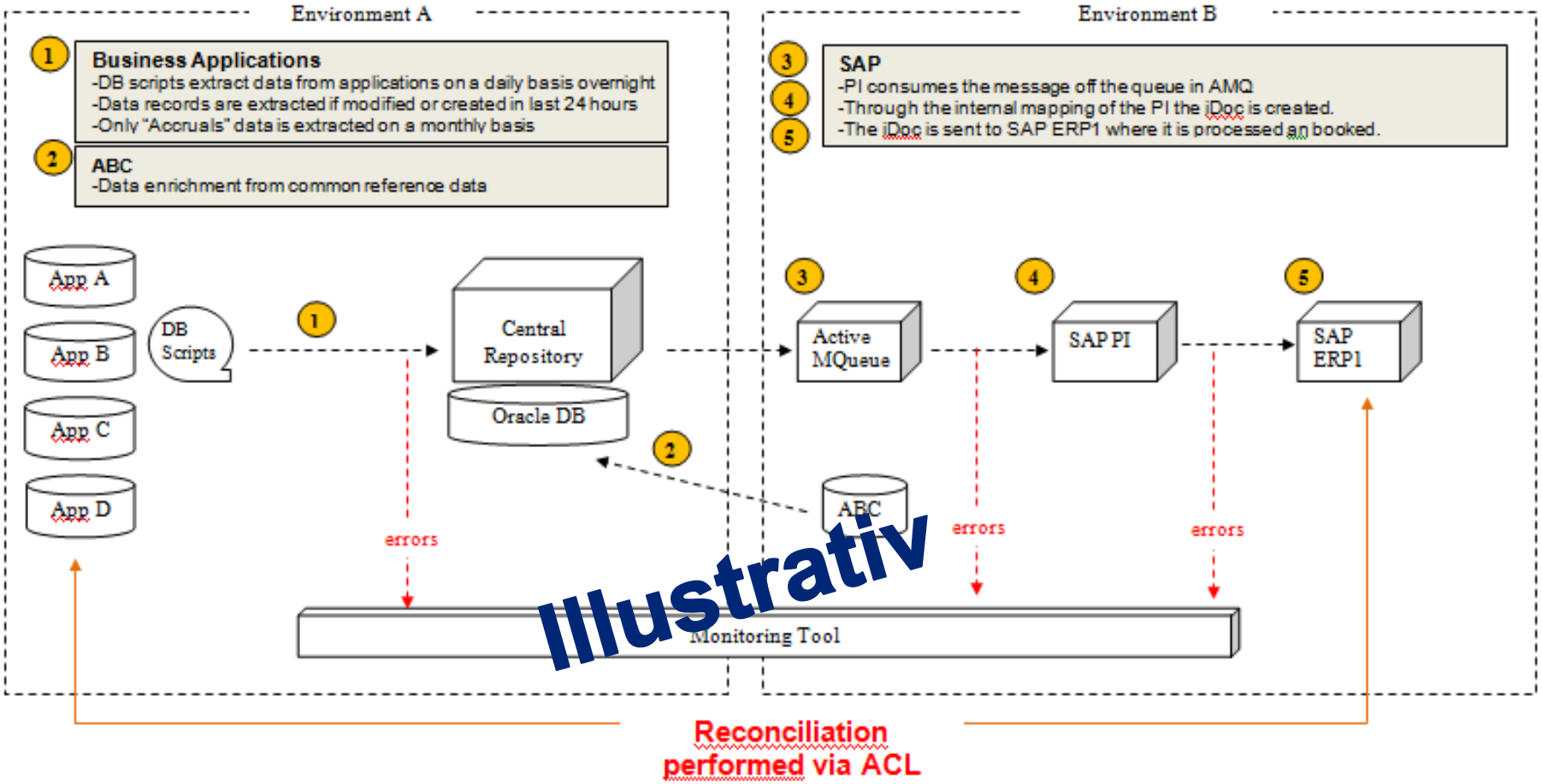
No.	*Control*	*Test of control*	*Responsible*	*Result*
C	**Reject List** ▪ No mapping of Application A with Application B account structure: error log. ▪ Problem when uploading data from Application B Upload table (5) to Application B production system (7): error log.	▪ Get a copy of last 5 Reject List. ▪ Review ▪ See follow-up of encountered errors: - communication between Fin. Dep. and IT - See error handling documentation	Finance department: Person x, IT department: Person y	See w/p xyz.
D	**Bank Balance Check Report** (comparing balances) ▪ Enforced daily print-out with Application A and Application B booking summary (BO report). Finance departments daily check: Identify reasons for differences, initiate corrections. ▪ Print-outs are filed.	IT inquiry & evidence: ▪ How is this report generated? ▪ What data is/is not selected? ▪ Review & test the script Finance inquiry & evidence: ▪ Get a copy of last 5 reports. ▪ Review ▪ See follow-up of encountered errors: - communication between Fin. Dep. and IT - Test error handling	Finance department: Person x, IT department: Person y	*Inquiry of XY (Finance) on xxx supported review by documentation.* **Bank Balance Check Report** ▪ Please refer to example xyz ▪ List of bank accounts with balance differences in Application A and Application B (error report) ▪ Report is generated automatically (no manual criteria selection by user). ▪ **Control procedures** Same as "Pending Reversals" → During monthly closing any balance differences would be detected as the latest and the Finance department would contact XY. ▪ **Interface problems** According to XY there have not been...

Beispiel 2: Prüfung von Kontrollen nach Go-Live gem. Standard-Prüfprogramm

SAP Interface Risk and Control Framework			
#	**Phase**	**Risk**	**Control**
1	Planning	Lack of a strategy or common approach to building interfaces may result in programs that are inconsistently developed and difficult to maintain and audit in the future.	An interface strategy document exists that provide guidelines on the planning, design, build, testing and deployment activities for interfaces.
4	Design	Lack of a strategy or common approach to building interfaces may result in programs that are inconsistently developed and difficult to maintain and audit in the future.	Standards, such as naming conventions for programs, files, and the data dictionary are being used. In addition, standards require that both the sender and receiver systems should have header records/control records which include at a minimum, date, record count, and hash totals. In absence of an IDOC interface, standard reports would have the required minimum information.
5	Build	Interface program do not provide efficient means to identify, track, and record errors in data transmission.	The interface program includes an error resolution routine that flags erroneous records and provides information on the errors encountered.
6	Build	Unauthorized Batch Input sessions could be created and processed which may lead to inaccurate or incomplete processing of data.	A system ID is set up to run the interface. The system ID is assigned a specific role with access restricted to run the interface only.
12	Testing	The interface does not meet business requirements.	The interface is integration tested. Test result exceptions are resolved appropriately.
13	Post go-live	Unauthorized Batch Input sessions could be created and processed.	The ability to run a batch job under another userid is restricted to authorized personnel.
16	Post go-live	Rejected data may not be corrected timely.	An authorized user will have the ability to repost files (IDOC or File Based transfer) with errors that are classified as either a Record Lock or Missing Reference. In the event of a Wrong Data type error, the error must be escalated to IT with the approval of the business process supervisor.
18	Post go-live	Duplicate or missing files would not be detected	A reconciliation between relevant records in SAP and other systems is performed by the business periodically. Any reconciling items are investigated and resolved in a timely manner.

Beispiel 3: Prüfung mit ACL

Interface process that extracts data from business applications overnight and books iDocs into SAP on a daily basis.



5. Zusammenfassung

Ausgangslage

Hypothese 1	Hypothese 2	Hypothese 3
„Die Prüfung von Schnittstellen zwischen ERPs und Umsystemen wird häufig vernachlässigt.“ 	„Die Prüfung von Schnittstellen bedingt vor allem vertieftes IT-Knowhow.“ 	„Stimmt das Total der Ausgangsdaten mit dem Total der Zieldaten überein, so kann nichts schiefgegangen sein“. 

Kernaussage

Die sinnvolle Prüfung von applikatorischen Schnittstellen bedingt v.a. eine gute Kooperation zwischen IT- und Fachrevision und muss sorgfältig geplant werden.

6. Fragen

Vielen Dank!

Deloitte.

Nathalie Lacambra, lic. oec. HSG
CISA, CIA
Senior Manager
Enterprise Risk Services

Deloitte AG

General-Guisan Quai 38
8022 Zürich
Switzerland

Tel.: +41 58 279 6482
Mobile: +41 79 215 8005

nalacambra@deloitte.ch
www.deloitte.ch

Member of
Deloitte Touche Tohmatsu

Deloitte.

Stefan Gröninger
Dipl. Wirtschaftsinformatiker (FH)
Senior Consultant
Enterprise Risk Services

Deloitte AG

General-Guisan Quai 38
8022 Zürich
Switzerland

Tel.: +41 58 279 6217
Mobile: +41 79 937 5460

sgroeninger@deloitte.ch
www.deloitte.ch

Member of
Deloitte Touche Tohmatsu