

MIS 5121: Business Processes, ERP Systems & Controls

Week 12: *Logs and Traces*

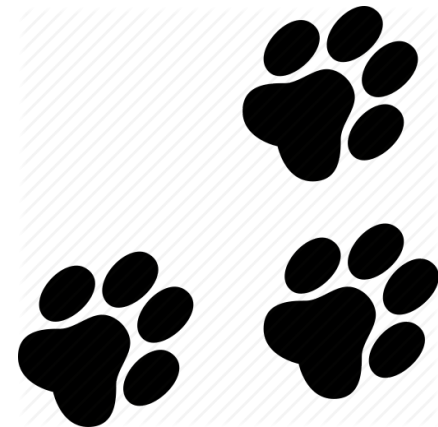
Key Information Technology Risks

- System Security
- Information Security Administration
- Data Migration
- Data Interface
- Instance Profile Security
- Change Management
- Transport Security
- Table Security
- Data Dictionary, Program and Development Security
- **Logs and Traces**
- Firefighter access
- Powerful User ID's and Profiles
- Background Processing (Batch vs. foreground: real-time)



SAP Integrated Change Log

- Built into most system documents (e.g. Sales Order, PO, Delivery, ...)
- Configuration to turn on/off some changes
- Data Stored in tables – available for subsequent reporting
- ‘Big Brother’ is watching?
- Excellent for problem diagnosis



Change Documents

- Change 'log' stores information on changes made to master data and transaction data via standard transactions (Miss direct table maintenance changes)
- Permanent record and audit trail for transactions executed in SAP

The screenshot displays the SAP 'Changes in Order 1' interface. At the top, there is a title bar 'Changes in Order 1' and a menu bar with buttons for 'Menu', 'Back', 'Exit', 'Cancel', and 'System'. Below the menu bar is the 'DocHeader' section. The main content area shows a table with the following data:

ID	Time	Sales Promotion	Old value	New value
<input type="checkbox"/>	16:48:45	Incoterms (Part 2) change	Miami	Tampa

Below this table, there is a smaller window titled 'Changes in Order 1' with its own 'DocHeader' section. This window displays a detailed table of the change:

Table	Field	User	TCode	Date	Time
VBKD	INCO2	GBI-002	VA02	04/03/2015	16:48:45

Risk and Recommendation

Change Documents

Risks:

If users are not restricted from maintaining change documents, the system audit trail from changes documents could be deleted accidentally or via malicious intent

Recommendations:

Users in production have activity level of security object S_SCD0 set to '08' (Display Change Documents).

Investigate ways access to maintenance of change documents could be further restricted (locking transaction)

System Logs and Traces

- Need to be activated to exist
- System Audit **Log** can be set up (SM19) to record:
 - ✧ Successful / unsuccessful Dialog logon attempts
 - ✧ Successful / unsuccessful RFC logon attempts
 - ✧ RFC calls to function modules
 - ✧ Changes to user master records
 - ✧ Successful / unsuccessful Transaction starts
 - ✧ Changes to the audit configuration
- System **traces** (ST01 / ST05) for:
 - ✧ Database access
 - ✧ ABAP/4 programs
 - ✧ Internal system activity
 - ✧ Developer traces
 - ✧ RFC Calls

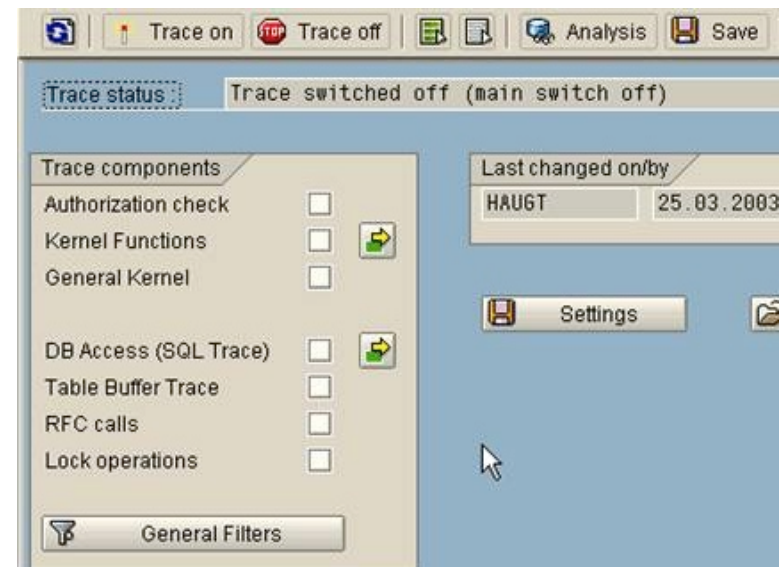
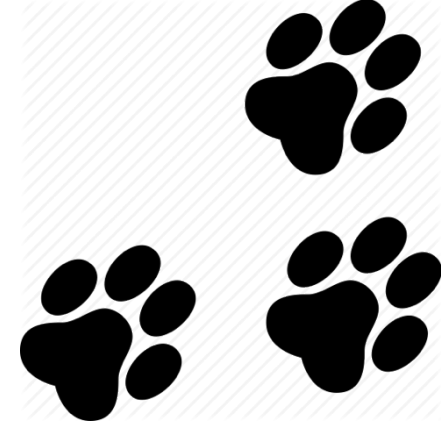


Table Logging

- In addition to system change logs supports traceability
- Needs to be activated in system to exist
- Can be activated individually by table via SE13
 - ✧ Concern: for high change rate tables logs fill up fast

The screenshot shows the SAP Dictionary: Display Technical Settings for table MARA. The interface includes a menu bar with buttons for Save, Back, Exit, Cancel, and System. The table name is MARA, and it is identified as a transparent table. The short description is General Material Data. The last changed date is 05/13/2014, and the status is Activated and Saved. The General Properties tab is selected, showing Logical Storage Parameters: Data Class is APPL0 (Master data, transparent tables) and Size Category is 4 (Expected data records 14,000 to 59,000). The Buffering section has three radio buttons: Buffering Not Allowed (selected), Buffering allowed but switched off, and Buffering Activated. The Buffering Type section has three checkboxes: Single Records Buff., Generic Area Buffered, and Fully Buffered. The Number of Key Fields is 0. A yellow button labeled Log Data Changes is visible at the bottom.

Dictionary: Display Technical Settings	
Menu	Save Back Exit Cancel System
Name	MARA transparent Table
Short Descript.	General Material Data
Last Changed	SAP 05/13/2014
Status	Actv. Saved
General Properties DB-Specific Properties	
Logical Storage Parameters	
Data Class	APPL0 Master data, transparent tables
Size Category	4 Exected data records 14,000 to 59,000
Buffering	
<input checked="" type="radio"/> Buffering Not Allowed	
<input type="radio"/> Buffering allowed but switched off	
<input type="radio"/> Buffering Activated	
Buffering Type	
<input type="checkbox"/> Single Records Buff.	
<input type="checkbox"/> Generic Area Buffered	
<input type="checkbox"/> Fully Buffered	
Number of Key Fields 0	
Log Data Changes	

Risk and Recommendation

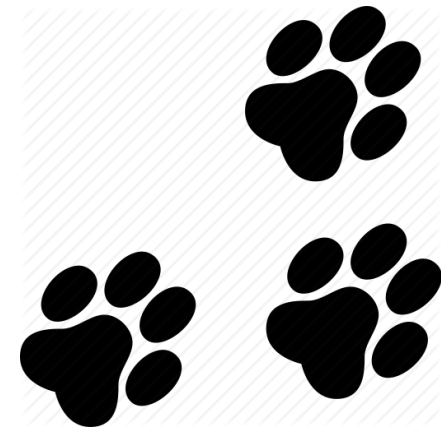
System Logs and Trace Files

Risks:

- If audit files (Logs and traces) are not secured at the operating system level for each application server, they could be maliciously deleted

Recommendations:

- Secure folders where log and traces files are stored at the operating system level
- Develop and use procedures for how to review and run traces at part of routine system security monitoring



Key IT Controls Overview

- Logs and Traces
 - 2-3 risks that exist
 - Common control recommendations for each

