MIS 5121:Business Processes, ERP Systems & Controls
Week 12: *Logs and Traces*

FOX | MIS
Management Information Systems

Edward Beaver
Edward.Beaver@temple.edu

ff

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
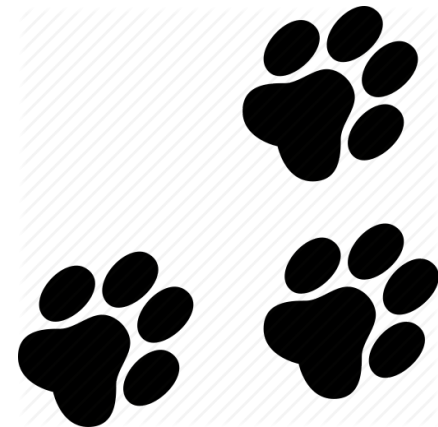
Change Documents

➢ 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

Changes in Order 1

| Menu | | ◄ | Back | Exit | Cancel | System |

DocHeader

ID	Time	Sales Promotion	Old value	New value
⬤	16:48:45	Incoterms (Part 2) change	Miami	Tampa

Changes in Order 1

DocHeader

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

| Trace on | 🛑 Trace off | | | 🔍 Analysis | 💾 Save |

Trace status : Trace switched off (main switch off)

Trace components			Last changed on/by	
Authorization check	☐		HAUGT	25.03.2003
Kernel Functions	☐	➡		
General Kernel	☐		💾 Settings	📂
DB Access (SQL Trace)	☐	➡		
Table Buffer Trace	☐			
RFC calls	☐			
Lock operations	☐			
🔻 General Filters				
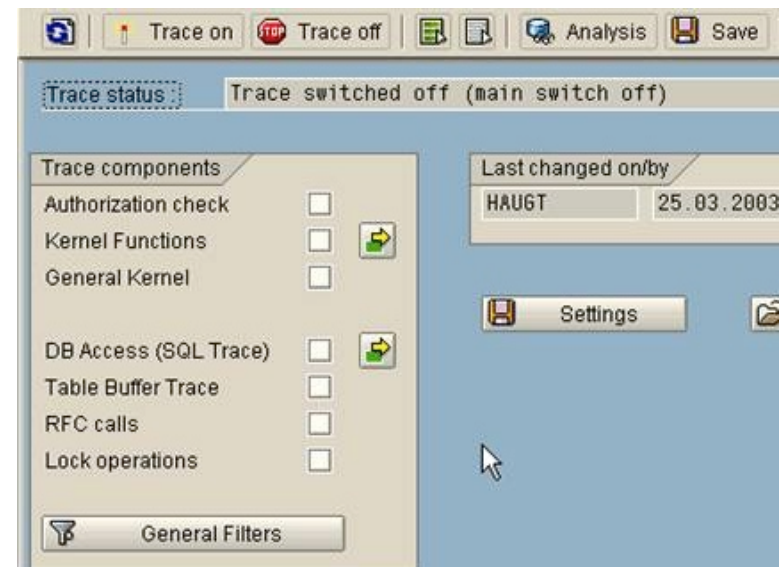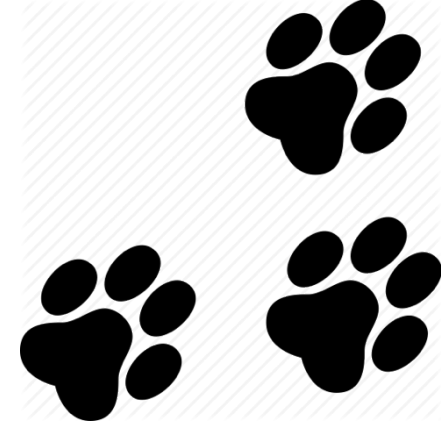
Table Logging

➢ 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
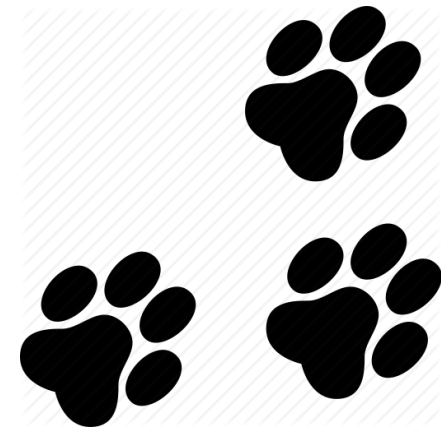
Risk and *Recommendation*
System Logs and Trace Files

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