Fraud Auditing within a SAP R-3 Environment

Phil Moulton CA CIA MBT
Business Audit Services Manager
Pauls Limited

Key Message

SAP can facilitate some types of frauds and deter others.

The challenge for the internal auditor working with SAP is to have the skills, imagination and knowledge to deter, detect and deal with fraudulent transactions.

At the end of this session you should (hopefully) have some very nifty tools to use once you go back to work.

Agenda

- What is SAP?
- SAP Audit Universe
- Fraud Auditing Basics (refresher)
- Assessing control environment - A/P
- Star Trek Auditing

What is SAP?

- An application drawing data from a DBMS
- Classed as an ERP system
- Configuration is very flexible
- Security Authorisation concept is ***very*** complex

What is SAP?

An important point to note is to realise that SAP is an application program, like Microsoft Excel or Word. It typically sits between the end user and a database management system (such as Oracle or Unix) and controls the recording, amending and reading of data from that database.

Classed as an ERP system: this means that it links data in real time across the traditional business functions such as sales-production-inventory-procurement-finance.

Configuration is very flexible: SAP is a very flexible system as the companies who have implemented it can tell you. The so called standard SAP configuration is often altered to suit the organisational needs and requirements. This adds to the complexity of auditing the system because not only do we need to know how SAP works but also how the particular company's system works.

One important characteristic of the SAP system is that where users go is dependent on their security authorisation profile - not their default menu screen. Unfortunately moving through the SAP security authorisation concept is a labourous affair but I will provide some useful tips during the course of this presentation.

The SAP Audit Universe

- Why is SAP different to other computer systems?
  - Complexity in implementation
  - Packaged and rolled out as a “total solution”
  - More access to both masterfile and transactional data
  - Challenged the role of middle manager

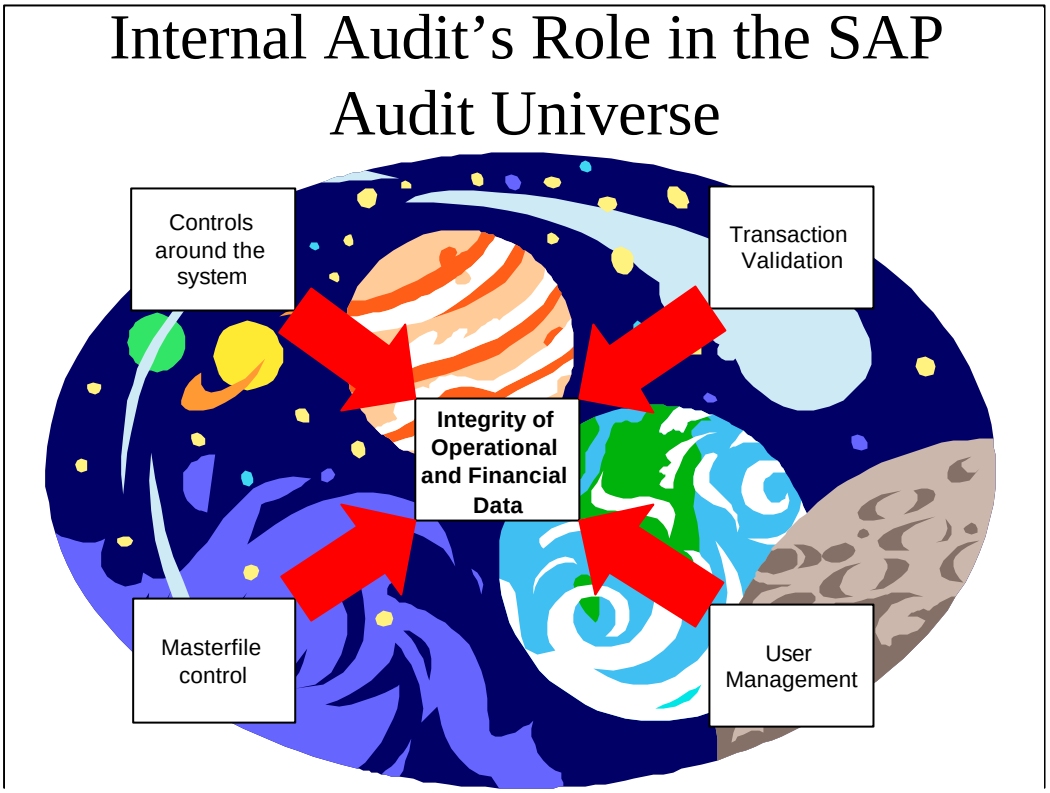
An important question to ask at this point is why is SAP different to other computer systems?

Firstly, history has shown that the implementation of SAP is typically very complex requiring an organisation to reflect on very fundamental questions such as how do we deliver value to stakeholders, and then designing business processes around that goal. It is not surprising then that SAP is typically introduced as part of an overall re-engineering project.

Going on from this point, the next important point to note is that it is typically packaged and sold as a total solution. This means that operational data and financial data are tied together so that more people are able to enter transactions which impact profitability without possible review or checking by a supervisor or manager.

Because of the complexity involved in the SAP Security Authorisation Concept, many organisations have tended to give very wide access to data without necessarily analysing the work requirements of the particular users. This obviously has a very pervasive impact on segregation of duties issues which I will talk about shortly.

Finally the role of SAP, along with the emergence of the business process paradigm, has challenged the role of the middle manager, middle management’s role in collating and reporting, review and authorisation has been substantially replaced by SAP and other ERP systems. This means that the questioning and follow up formerly done by middle managers is probably not as substantial as it once was.



This is the way my audit team looks at auditing in an SAP universe

User management

- Security authorisation issues
- Redundant user identification
- Superuser management
- Profile design
- Password control

Controls around the system

- Reconciliation of control accounts to subsidiary ledgers – accounts payable, accounts receivable
- Reconciliations of SAP data to external information – bank reconciliation, accounts payable statement reconciliations
- Cost centre and responsibility accounting
- Management review and budgetary control
- Review and authorisation of non-routine transactions

Validation checks

- Validation of data input in particular transactions
- Properly designed ABAP statements with authority checks
- Matching of documents prior to "closing out" eg purchase order – receiving documentation – invoice

Masterfile control

- Independent review of masterfile changes
- Independent masterfile creation to transactional responsibilities

Identifying redundant master

Fraud Auditing Basics

- Red flags and indicators
- Fraud Triangle
- Off book and on book fraud
- Fraud within SAP is going to be “on-book”

Fraud Auditing Basics

Now that I have given you a taste of my approach to auditing in an SAP environment, let me move onto fraud auditing.

When we want to audit an area for fraud I go back to basics. In this respect, what I am looking for are red flags or indicators that fraud or some kind of irregularity is going on. Red Flags by themselves do not prove a fraud they are just an indicator. I will demonstrate use of red flag theory in the Purchasing and Accounts payable section in my presentation shortly.

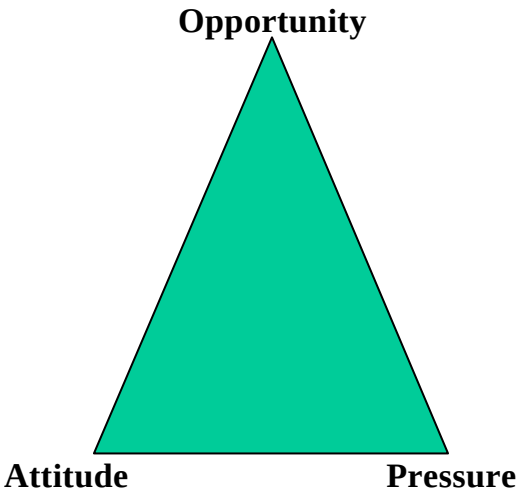
I am sure that many of you are familiar with the Fraud Triangle. Basically this represents the factors that enable a fraud to occur.

There are generally two types of fraud:

Off book - where the fraud is not required to be covered up eg corruption or payback schemes

On book - where the records are falsified to facilitate the fraud eg ghost employee

Fraud Triangle



Fraud Auditing Basics

What the Fraud Triangle represents is that the three elements of opportunity, attitude and pressure need to be present in order for a fraud to occur.

Pressure may mean an inability to pay debts (financial troubles); opportunity may mean lax internal controls over a certain area and the attitude is typically a rationalisation that says “it is ok to steal from my employer/the company etc.”

Obviously we cannot really effect attitude and pressure, but we as auditors have a responsibility to minimise opportunities by ensuring that internal controls are adequate to deal with the common types of frauds and irregularities.

If internal controls were a bit lax in an area, then the next step would be to consider red flags.

Identifying Red Flags

- A red flag is an indicator that something may be wrong, not necessarily proof
- Need to determine what “rules” are needed eg inventory and sales entries

As I indicated earlier, a red flag is not necessarily proof but simply that something looks wrong.

Before we start looking at an area we need to determine what “rules” or hypothesis we are going to use in order to define our fraud auditing testing. I am not telling you how to suck eggs but obviously we need to plan our approach, particularly in dealing with such a complex system such as SAP.

Some example of rules include:

•actual expenses far exceeding budgeted expenses and last years

•blow out in certain types of expenses

•significant manual journals being made to stock accounts and period end accounts

•addresses, telephone numbers and other data which link employees to firms which provide the organisation with goods and services’

•analytical ratios are not making sense: ratio of overtime expenses to sales, gross margins fluctations etc

•unexplained price increases in material costs (kickback scheme)

Examples - Compiling Rules for Fraud Auditing in SAP

- Stock and sales entries are system generated
- Each type of transaction - Document Type
- Fraud Test: Search for document types <> RE (Invoice receipt type) in GL account 200000 (Sales)
- Fraud Test: Search for document types <> WL (Goods Issue/delivery) in GL account 300000 (Cost of sales)

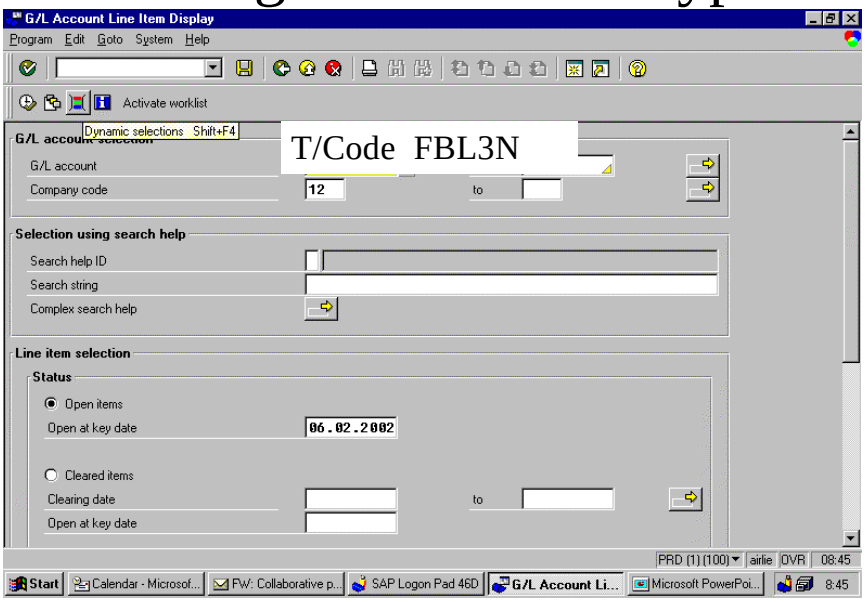
Fraud Auditing Basics

In SAP, stock and sales entries should be system generated which in turn gives us standard document types

The challenge is then to use these standard document types to assist us in our fraud auditing efforts

One example…. (third bullet)

Searching for document types

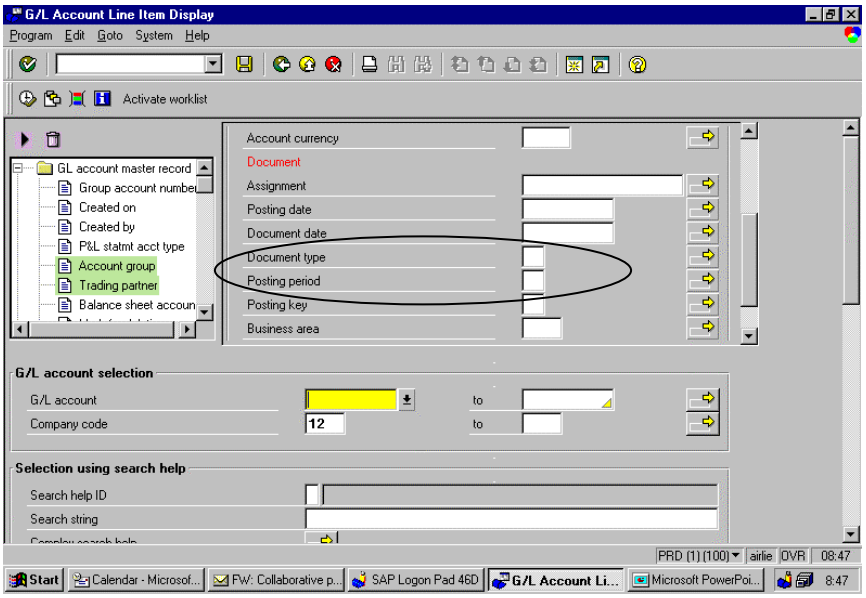


Fraud Auditing Basics

How do we do this?

The answer lies in transaction code FBL3N and utilising the dynamic selection button.

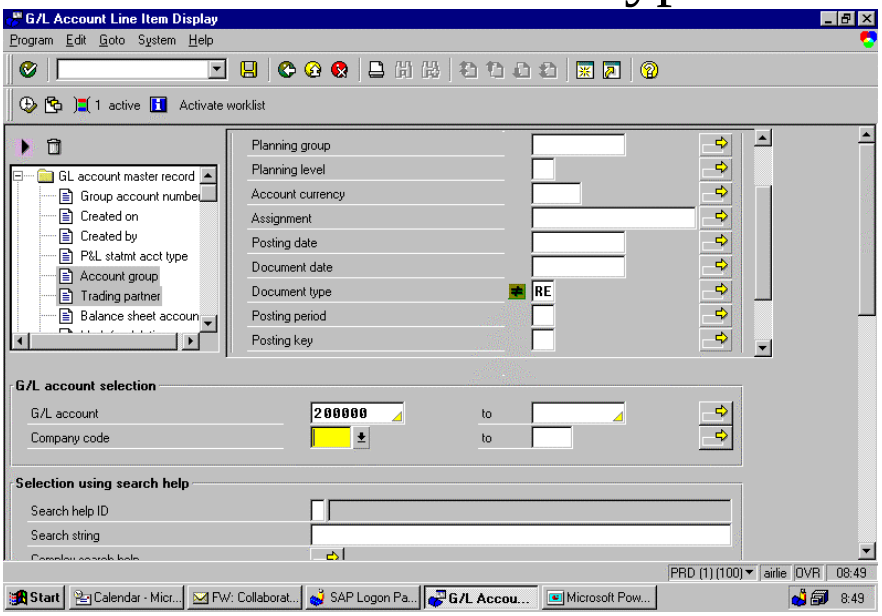
Dynamic Selections



Fraud Auditing Basics

We can now defined the document type as well as the GL account.

Exclude document types



Fraud Auditing Basics

In this case I want SAP to give me a listing of all document types <> RE that appear in account 200000. In other words - SAP, I want you to give me a list of all non-system generated sales documents that have been posted to the revenue account.

Accounts Payable in SAP

- A/P generally is the predominant source of frauds
- In built controls - SAP
- In built risk - SAP

Assessing the Control Environment - A/P

I would now like to move onto SAP specifically and discuss fraud in this area.

As an accounting transaction cycle, purchasing and accounts payable represents a major area for fraud (around 70%). You don't need to be an Einstein to know why - the cycle results in the physical disbursement of cash to suppliers for goods/services that have been recorded in the books and records of the organisation.

It is appropriate here to discuss what in built controls SAP has to avoid fraudulent activity in the accounts payable function:

- Three way check between PO-GR-Invoice to a given threshold
- Vendor Masterfile change reports
- Check double invoice control - the system will review invoices posted to a particular vendor code and highlight whether the current invoice is the same as a previous one.
- Primary risks involved with SAP Accounts payable:
- Use of one time vendor code
- Authorisation too broad (segregation of duties issues)
- Payments going through FI-AP are generally more risky than MM-AP due to lack of purchase order
- Name3 field is often used as the field which is used for writing the payee on the cheque

SAP Accounts Payable Fraud Audit

- Assess the risk
  - Review levels of RE documents versus KR versus ER
  - Review use of one-time vendor accounts
  - Use of external systems
  - Assess Segregation of Duties

Assessing Control Environment - A/P

Moving along to identifying potentially fraudulent payments, as with any audit, I would start out with some analytical tools which may indicate to me some red flags and the overall risk in the area.

With Accounts payable, generally there are three types of payments transactions - payments which have come through on purchase order, payments which are paid by invoice and payments which have been made through a evaluated receipts program which may have been kicked off by a DME upload of an Excel file generated outside SAP.

I would also like to know what is the extent that the One-time vendor code is being used? The one time vendor code is set up so that a payment can be processed without having to set up a vendor masterfile. As its name suggests, it is supposed to be used for the one off payments to particular vendors who we do not generally do business with. If there are payments being made through the account to a particular vendor, then you would have to ask the question why a vendor masterfile has not established.

We need to assess segregation of duties. If the segregation of incompatible duties is strong within an organisation, then the risk of fraud is lowered and further work can be conducted on that basis.

Lets talk about how to assess segregation of duties in SAP.

Assessing segregation of duties - A/P in 7 Easy Steps

Objective

Identify users with incompatible duties:

- purchasing,
- goods receiving,
- invoice processing and
- cash disbursement responsibilities

Step 1

Identify how your organisation processes payments- usually: Raise PR - Release PR - Raise PO - Release PO - Goods receipt

- Enter invoice - process payment

Step 2

Identify the relevant transaction code for each step by reviewing the standard menus

Ask the accounts payable staff and purchasing staff what standard menus they use.

Step 3

Identify key control points: Raise PO, Release PO, Goods receipt, enter invoices, create and change vendor masterfiles

What are the key transactions?

Assessing the Control Environment

Recall that when we are dealing with internal control evaluation, some controls and transactions are more significant than others.

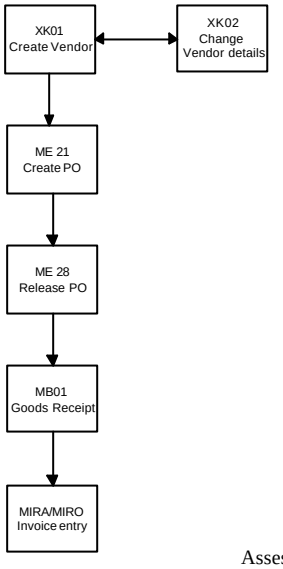
Step 4

Identify other incompatible duties: regular payment processing and vendor masterfile responsibilities

Step 5

Identify your rules - convert to “SAP speak”

Converting rules to SAP speak



- Examples:
  - XK01/XK02 <> ME28
  - ME21 <> ME28
  - ME28 <> MB01
  - XK01/XK02 <> MIRA/MIRO

Assessing segregation of duties - A/P (continued)

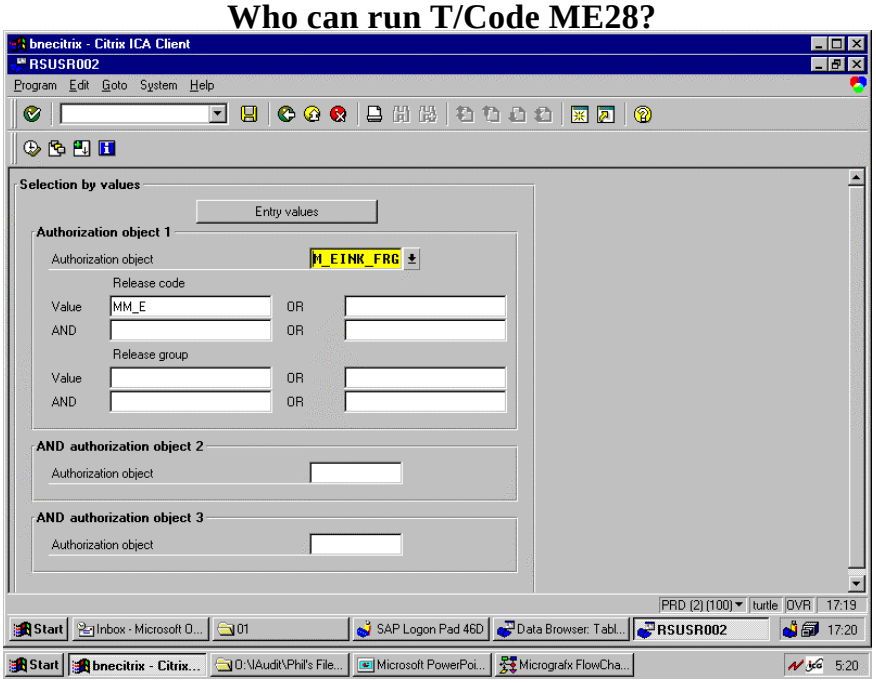
- Transaction codes = Authorisation objects in Table TSTCA
- ME28 = Object: M_EINK_FRG, object class: MM_E.
- Now run program RSUSR002

Point 1: an alternative is to try the transaction yourself and obtain the authorisation check statement

from Table TSTCA, I can see that to run transaction code ME28 - Purchase order release - I need the authorisation object M_EINK_FRG and have the value MM_E somewhere in my user SAP authorisation profile.

The next step is to identify the users who have this authorisation.

Who can run T/Code ME28?

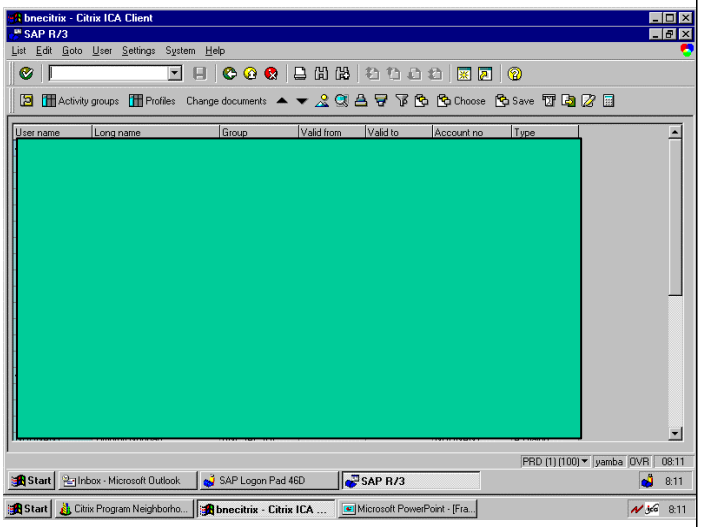


Assessing the Control Environment - A/P

You can obtain this screen by selecting SE38 and entering RSUSR002 or access the program via the Audit Information System

Employee database match

- Listing of employees with access to the transaction



Assessing the Control Environment - A/P

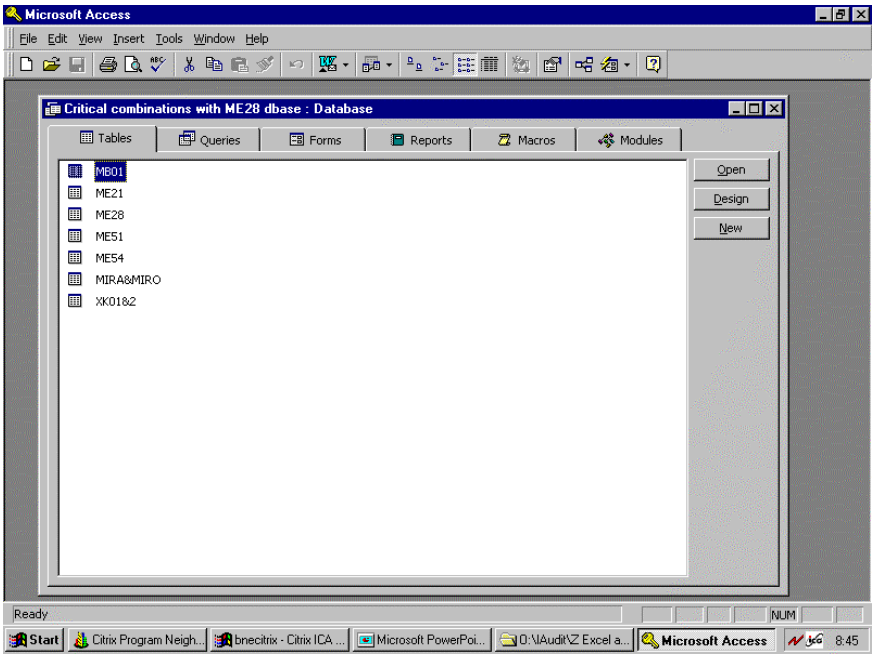
This is an actual list of people which I have covered up.

Step 6 - Find employees with incompatible duties

- Join employee lists utilising Microsoft Access by incompatible transactions
- This process may lead to further analysis of authorisation profiles (too broad?)

Some standard authorisation profiles in SAP are too broad from an auditor's point of view. We will discuss these shortly.

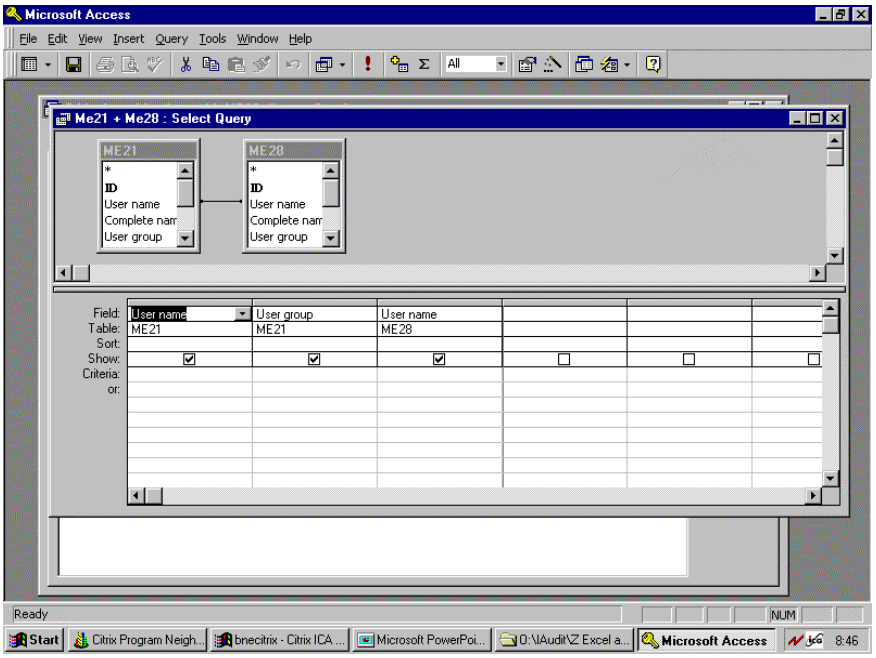
Export list to an Access Table



Assessing the Control Environment - A/P

Here is a listing of all the tables, I have named each table in accordance with the transaction code that I want. From here we can perform table joins using the query function

Join tables to identify users



Assessing the Control Environment - A/P

This query will now give me the usernames of people who have access to both ME 21 (Create purchase order) and ME 28 (Release purchase order).

This listing should then further analysed as to who is on the list and whether there are substantially any risks.

Are there any questions on determining segregation of duties?

Identify high risk vendors and payments

- Service accounts (tangible versus intangible deliverables)
- Match addresses and telephone numbers of vendors and employees - for this we can use a very nifty tool in SAP called...

Assessing the Control Environment - A/P

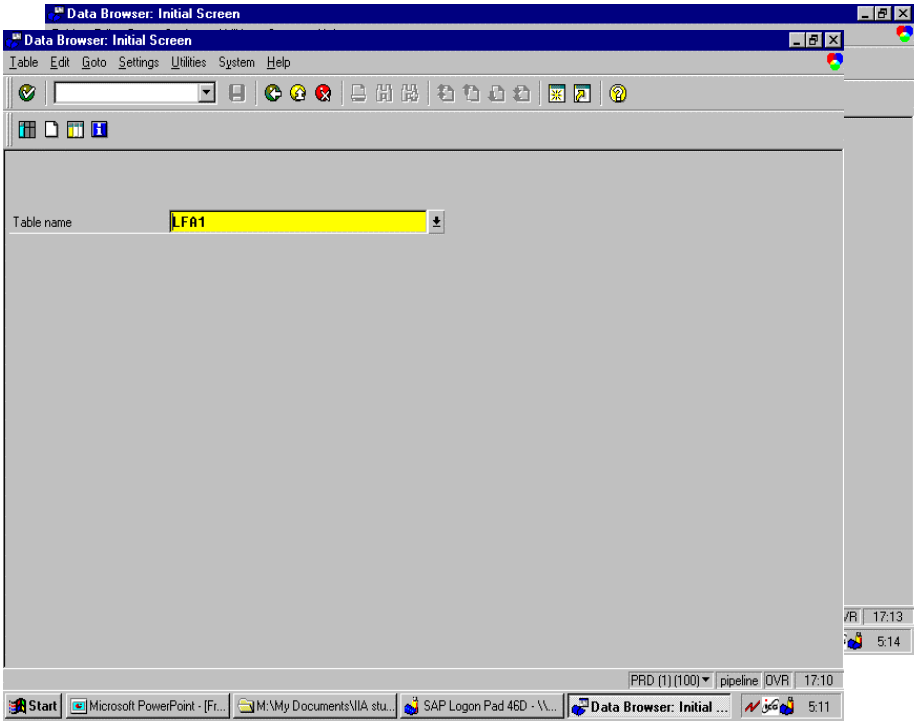
Another aspect of fraud auditing in Accounts payable and purchasing is identifying the typical places were fraudulent transactions are recorded.

These are typically recorded in service type accounts - generally not fixed assets or stock. Why. Will if I am a fraudster and record a phony transaction against stock or fixed assets, I generally have to have something to show for it right? In addition, if I work in a large organisation, I will have the asset accountant or stock controller on my back. So typically the fraudster will record something to a service type of account - consulting, advertising, marketing tend to be utilised.

Use of SE16 Table Browser

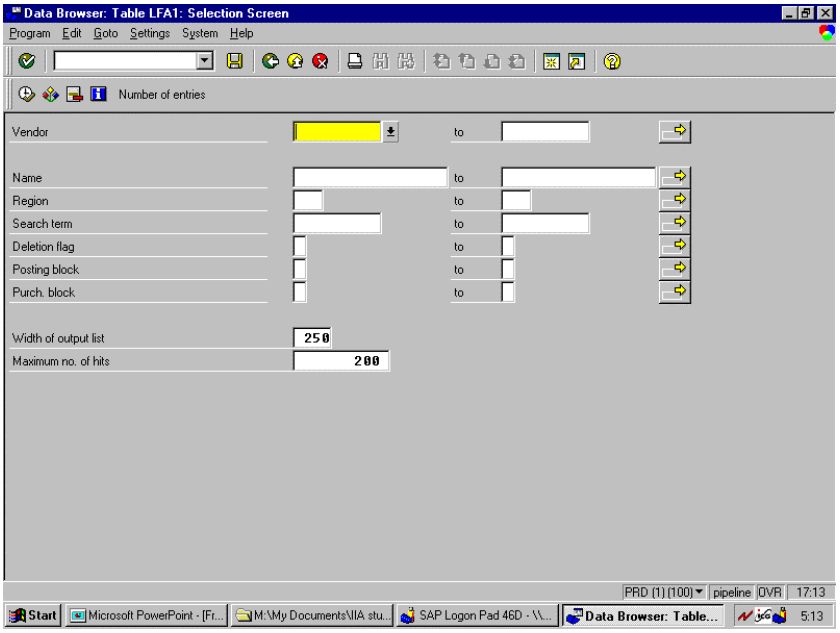
- Transaction code SE16 allows direct access to data tables
- Key tables - Accounts payable:
  - LFA1 - Name, contact details, ABN, etc
  - LFB1 - Payment terms, creation details, check double invoice control
  - LFC1 - Transactional information - debits and credits etc

SE16 Table Browser



The SE 16 Table browser looks like.

You put in a known table into the field



Assessing the Control Environment - A/P

The next screen allows me to enter * in the vendor field. This will allow me to list all vendors. I can then play around with the output screen to get it the way I want it to look.

We can do the same for employees and match them up using Microsoft Access.

Where can do the same for employee addresses (table PA0006) and match them using a Microsoft Access Query.

Star Trek Auditing

Going where
no auditor
has gone before.

Star Trek Auditing

- New skill sets
- Auditors can really shine with some basic SAP audit skills
- When it comes to hunting down fraudulent transactions, imagination, as well as knowledge is essential

Star Trek Auditing

SAP has challenged the role of internal auditors and it requires IA to learn new skill sets - some of which are fairly technical.

Hopefully your department can get to the point where senior management will say “whew, thank God we had Internal Audit pick up these things in SAP.”

One area which is generally quite ripe for internal audit involvement is assessing security authorisation profiles.

Global Authorisation Issues

- Powerful systems authorisations
- Powerful accounting authorisations

Powerful systems authorisations

- S_Develop
- S_USER_ALL
- SAP_ALL
- SAP_NEW
- S_ENT_W
- Who has access to: SU01 (create users), SU02, SU03 (authorisation maintenance), SE38 (access direct to SAP program)

Star Trek Auditing

Some very powerful systems authorisations include these ones. You should determine who has access to them - they should generally be limited to a small group of SAP administrators or systems user.

Some examples of powerful accounting authorisations

- ZF_ASSET_ALL, A_ALL - all asset accounting profile
- C_PPPI_ALL - all process manufacturing
- F_BUCH_ALL - All maintenance for FA
- F_KBE_TRA_A - All authorisations for payment transfer
- P_ALL - All HR authorisations
- V_SD_ALL - All SD Authorisations

Star Trek Auditing

In terms of accounting authorisation profiles, you should ensure that these standard SAP profiles are only available to a limited number of users - Probably more at manager level.

Conclusion

- SAP can perpetuate frauds + used as a tool
- Most significant fraud risk relates to system access and authorisation

Conclusion

SAP can perpetuate frauds but can also be used as a tool to hunt down misstatements and certain “on book” fraud schemes.

The biggest risk relates to access and system authorisation. Why?:

1. System authorisation concept is very complex

2. Relative lack of people with technical expertise here in Australia with a SAP background who understand segregation of duties concepts

3. Often the easiest answer is to give personnel very wide access rather than to work and tailor their access to their jobs. Otherwise if authorisations are set too narrow, users will end up hassling Help Desk resources.

4. We need as internal auditors to appreciate the pressures that the typical IT department have to deal with. The pressure to go live with new software (esp SAP which comes at great cost) can be immense. The pressure is on to put a functional system up and going, with it appearing on people’s desktops. System security issues tend to considered later, in talking with IT system consultants these issues may not be considered at all until they come in and perform a review.

Any questions?

How do I determine which tables to find?

How do I access SE38 Program?

We are upgrading shortly - any hints?

Should ensure the following:

•Change management and training

•Business process re engineering

•poor project planning

•underestimating resources

•poor executive buy in

•insufficient software selection

•lack of consideration of strategic matters

•Bottom line: It is the people issues rather than the technical which tends to cause project failure.

•Technical issue: Manually designed security profiles may not work in the new 4.6 environment. The new version has greater B2B functionality, particularly with purchasing. Clearly there is a dire need for someone with risk and controls expertise to be involved in this area.