सत्यमेव जयते

# Fraud Vulnerability Assessment in SAP Environment

## Case Study


**Indian Audit & Accounts Department**

**Regional Training Institute**

**26/1, Civil Lines, Nagpur**

***E-mail : rtiaadnr_ngp@sancharnet.in***

**Phone : (0712) - 2545420, 2545816, 2545829**

**Fax : 0712-2562577**

## CONTENTS

## 1. Fraud Vulnerability Assessment-background

1.1 Techniques for the assessment and examination of fraud differ considerably from those traditionally used in financial statement auditing. To begin an examination, a fraud examiner makes an *assessment* to determine if sufficient predication exists to commence a fraud examination. The Association of Certified Fraud Examiners defines predication as:

*The totality of circumstances that would lead a reasonable, professionally trained, and prudent individual to believe a fraud has occurred, is occurring, and/or will occur.*

1.2 This *assessment* is what may commonly be referred to as a fraud audit. If the fraud examiner finds sufficient predication as a result of the fraud audit, he or she will then begin a fraud examination. In the fraud examination, the examiner follows what is known as the *Fraud Theory Approach,* including the following steps:

- Analyzing available data
- Creating a theory or assumption
- Testing the theory
- Refining and amending the theory as necessary

## 2. SAP Environment

2.1 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: The standard SAP configuration is often altered to suit the organizational 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.

2.2 One important characteristic of the SAP system is that where users go is dependent on their security authorization profile - not their default menu screen. Unfortunately moving through the SAP security authorization concept is a laborious affair but there are some useful tips as this case study advises.

2.3 The organization introduced SAP in October 2004 by migrating from the earlier legacy system. There were about 300 users.

## 3. SAP Vs. other Computer systems

3.1 Firstly, history has shown that the implementation of SAP is typically very complex requiring an organization 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.

3.2 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. Further, 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.

3.3 SAP can facilitate some types of frauds and deter others. The challenge for the auditor working with SAP is to have skills, imagination and knowledge to deter, detect and deal with fraudulent transactions. Adequate segregation of duties among the users is the key concern since access to a combination of certain core functions can virtually give access to entire system to the users with such access. It is therefore essential that the management allocate the roles to the users on the 'need to know' or 'need to do basis'. Management's concern always remains smooth functioning of the process and getting the desired MIS. In this scenario internal controls of the system unknowingly take a back seat.

## 4. REVIEW OF INTERNAL CONTROL ENVIRONMENT

4.1 The organization's control environment is the foundation of all components of an effective internal control system. Commonly referred to as the "tone at the top," the control environment sets the tone for the organization and influences the control consciousness of its people. Effective internal control is perhaps the most important deterrent to fraud. Strong internal control can prevent or detect most types of fraud, waste and abuse. During our assessment of the current system of internal control, not only were we concerned with the controls in place but just as importantly whether those controls were operating as prescribed. As we identified fraud exposures and controls in a given area, we created procedures to test for compliance.

4.2 Effective segregation of duties, being one of the most important internal control mechanism for aversion of frauds the team focused on the extent and effectiveness of duties segregated.

## 5. SCOPE OF AUDIT

5.1 Management requested the external auditors to give assurance on, among others, the following issues of the system.

*5.2* Tests of security, authorizations and segregation of duties within SAP

- Review of the use of roles to control access within SAP
- Review of role assignments to identify conflicts or issues with segregation of duties
- Restriction on powerful transactions

*5.3* Our work in this matter conducted in October 2006 covered the period from January 1, 2006 through August 31, 2006.

## 6. METHODOLOGY

**Segregation of duties-key to prevent frauds in SAP.**

6.1 We began with obtaining an understanding of the systems and procedures which were in place in the SAP system. Discussions were held with the Management as well as the Internal Audit & Oversight. It is this understanding which provides the basis for the assessment of the internal control structure, the identification of fraud exposures and the evaluation of fraud symptoms.

6.2 Considering adequate segregation of duties reinforce the strength of internal controls and act as a defense shield against any fraud, the focus was on vulnerability to fraud through assessing the strength of segregation of duties and access to powerful transactions in the system.

6.3 Access control forms a very important part of the overall control framework in any ERP environment. In SAP R/3 segregation of incompatible functions is a major control point. Assessing whether incompatible functions are assigned to SAP users individually was a tedious task before the team. So how did we go about addressing such incompatibility issues? It is explained with an example of the accounts payable process in SAP. Ideally, in A/P segregation of duties should exist between purchasing, goods receiving (GR), invoice processing and cash disbursement functionalities.

6.4 As explained below, I have followed the following given 9 step process for segregation of duties in SAP Accounts Payable.

**Step 1** - Document the entire process of payables. This included raising a purchase requisition, releasing purchase requisition, raising a purchase order (PO), releasing purchase order, goods receipt, invoice entry, and finally processing payments.

**Step 2** - For each of the sub-process identified above, identify the relevant transaction code in SAP. This was done using the standard menus in SAP.

**Step 3** - Identify the key control points within the process. In our example above, key control points was raise PO, goods receipt, enter invoice, create and changing vendor master records.

**Step 4** - Identify if there are any other incompatible duties. One such incompatible function would be payment processing and vendor master maintenance.

**Step 5** - Identify the transaction codes in SAP which allow access to these incompatible functions or set the rules detailing the incompatible function duties. Now in SAP the relevant transaction codes would be: XK01 / XK02 - Create Vendor / Change Vendor details, ME21 - Create PO, ME28 - Release PO, MB01 - Goods Receipt, MIRA / MIRO - Invoice Entry. The incompatible functions relevant for segregation of duties would be a combination of functions as detailed in the rules set below by the Auditor.

| Tcodes (Combination of) | Users have access to |
|---|---|
| **Rule 1** | |
| me51n | create_purchare_requisition |
| me21n | create_PO |
| me29n | release_PO |
| mk01 | vendor_master_creation |
| miro | vendor_invoice |
| migo | goods_receipt |
| f110 | payment_run |
| fk01 | finance_create_PO |

| Rule 2 | Description |
|---|---|
| me21n | create_PO |
| me29n | release_PO |
| mk01 | vendor_master_creation |
| miro | vendor_invoice |
| migo | goods_receipt |
| f110 | payment_run |
| fk01 | finance_create_PO |

| Rule 3 | Description |
|---|---|
| mk01 | vendor_master_creation |
| miro | vendor_invoice |
| f110 | payment_run |

| Rule 4 | Description |
|---|---|
| miro | vendor_invoice |
| f110 | payment_run |
| me21n | create_PO |

| Rule 5 | Description |
|---|---|
| me21n | create_PO |
| mk01 | vendor_master_creation |

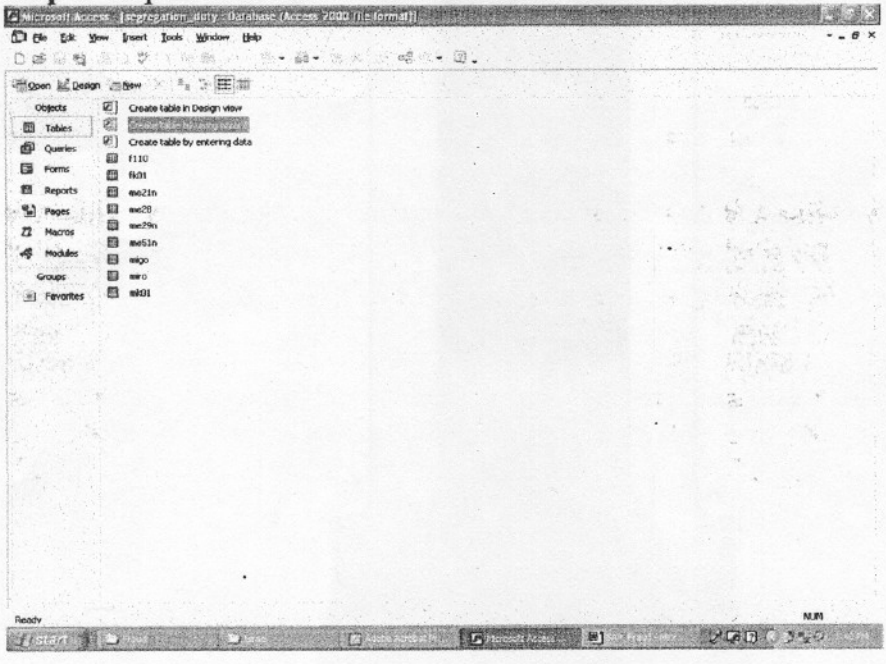
| migo | goods_receipt |
|---|---|

**Step 6** – The next question after setting the above rules is-how many users have access to this kind of combination of duties? Therefore, identify the employees within the organization who have access to such incompatible functions. This was done using SUIM, data analysis tools. If required analysis can be even done at the authorization profile level. There were about 300 users in the organization, out of which about 225 were active users.

**Step 7-** Find employees with incompatible duties

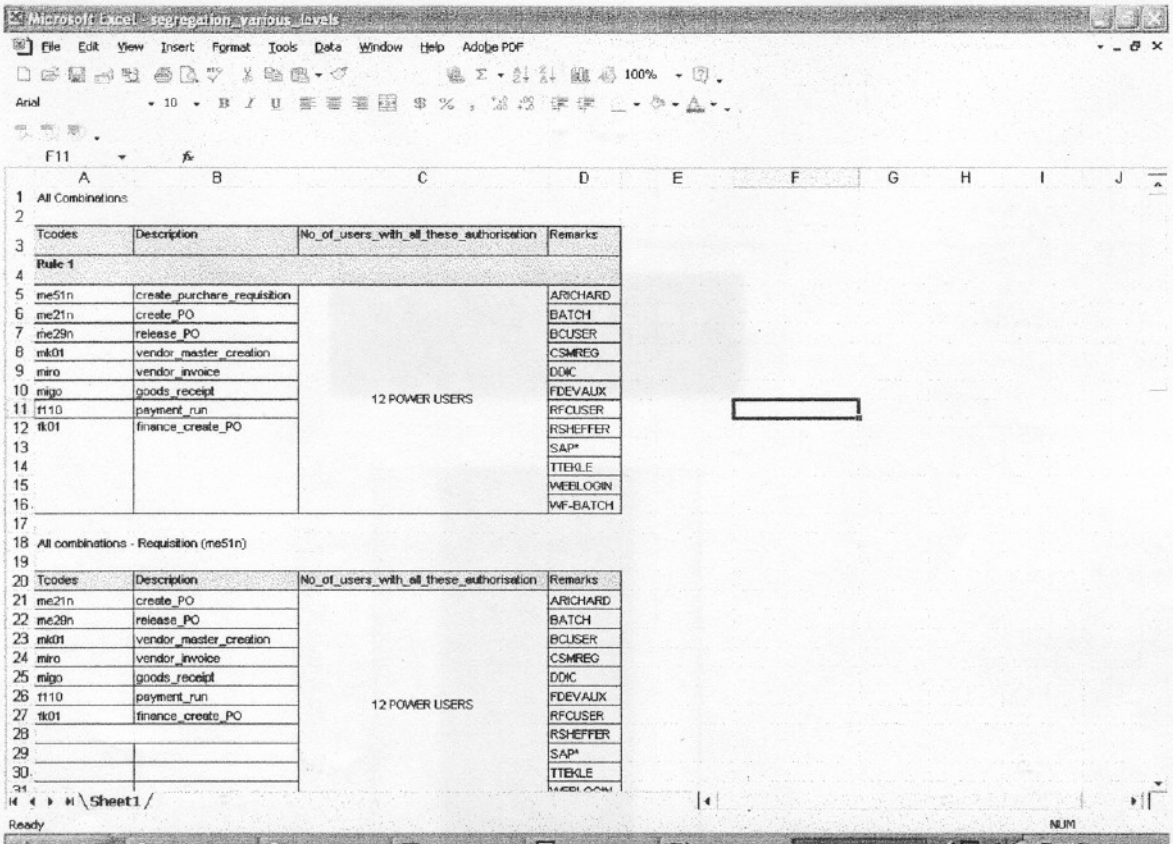
- Join the lists for each authorization generated through SAP utilizing Microsoft Access by incompatible transactions.
- This process may lead to further analysis of authorization profiles (too broad?) Some standard authorization profiles in SAP are too broad from an auditor's point of view.

**Step 8-** Export list to an Access Table as detailed below.




**Step 9-** Now, join the tables to identify users

This gave the usernames of people who have access to different combinations of access as detailed below. Thereafter a summarized a general profile as indicated at the end of the case study indicating the T-code, its description, number of users having access to the authorization, risks involved and suggestions.



Microsoft Excel - segregation_various_levels

File Edit View Insert Format Tools Data Window Help Adobe PDF

F11

All Combinations

| Tcodes | Description | No_of_users_with_all_these_authorisation | Remarks |
|---|---|---|---|
| **Rule 1** | | | |
| me51n | create_purchare_requisition | 12 POWER USERS | ARICHARD |
| me21n | create_PO | | BATCH |
| me29n | release_PO | | BCUSER |
| mk01 | vendor_master_creation | | CSMREG |
| miro | vendor_invoice | | DDIC |
| migo | goods_receipt | | FDEVAUX |
| f110 | payment_run | | RFCUSER |
| tk01 | finance_create_PO | | RSHEFFER |
| | | | SAP* |
| | | | TTEKLE |
| | | | WEBLOGIN |
| | | | WF-BATCH |

All combinations - Requisition (me51n)

| Tcodes | Description | No_of_users_with_all_these_authorisation | Remarks |
|---|---|---|---|
| me21n | create_PO | 12 POWER USERS | ARICHARD |
| me29n | release_PO | | BATCH |
| mk01 | vendor_master_creation | | BCUSER |
| miro | vendor_invoice | | CSMREG |
| migo | goods_receipt | | DDIC |
| f110 | payment_run | | FDEVAUX |
| tk01 | finance_create_PO | | RFCUSER |
| | | | RSHEFFER |
| | | | SAP* |
| | | | TTEKLE |
| | | | WEBLOGIN |
| | | | WF-BATCH |

Vendor_master_creation_and_vendor_invoice_entering_and_payment_run

| Tcodes | Description | No_of_users_with_all_these_authorisation | Remarks |
|---|---|---|---|
| mk01 | vendor_master_creation | 12 POWER USERS | ARICHARD |
| miro | vendor_invoice | | BATCH |
| f110 | payment_run | | BCUSER |
| | | | CSMREG |
| | | | DDIC |
| | | | FDEVAUX |
| | | | RFCUSER |
| | | | RSHEFFER |
| | | | SAP* |
| | | | TTEKLE |
| | | | WEBLOGIN |
| | | | WF-BATCH |

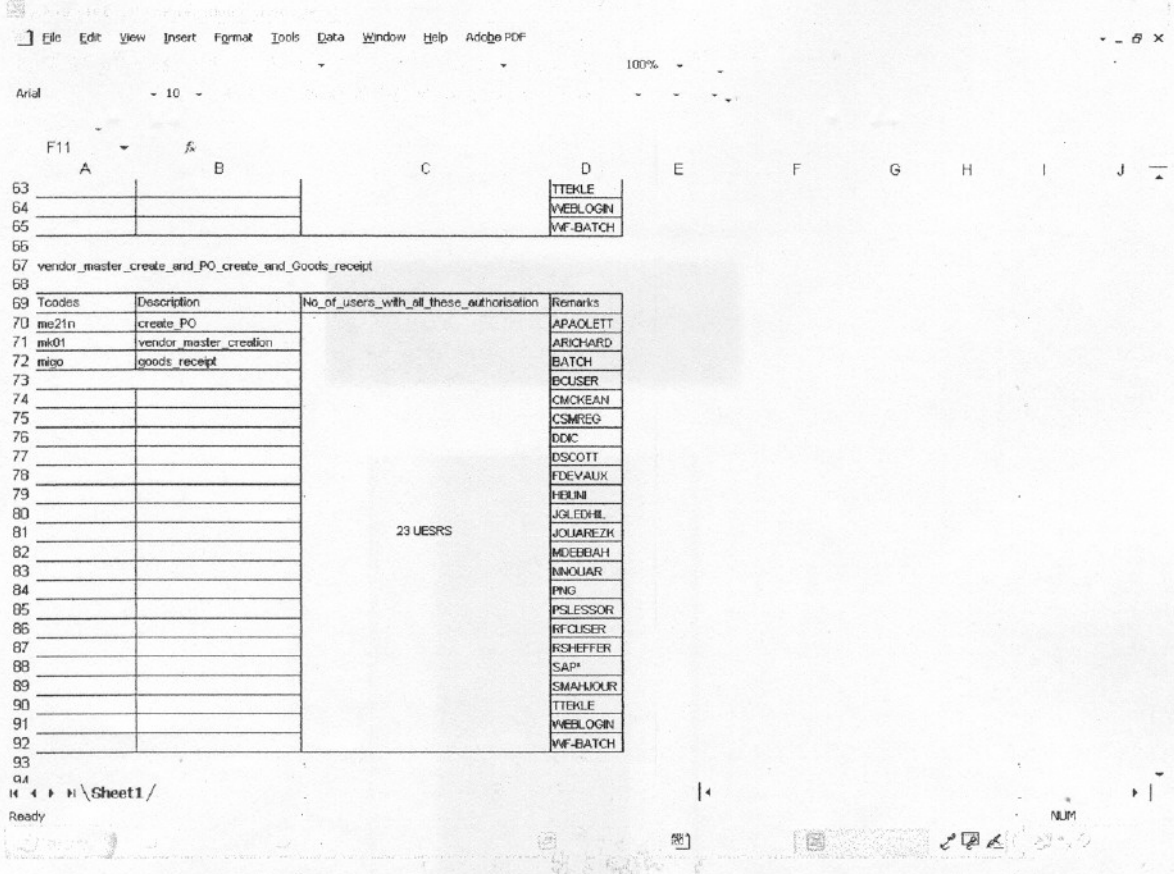
Purchase_order_creation_Vendor_invoice_entering_and_payment_run

| Tcodes | Description | No_of_users_with_all_these_authorisation | Remarks |
|---|---|---|---|
| miro | vendor_invoice | 12 POWER USERS | ARICHARD |
| f110 | payment_run | | BATCH |
| me21n | create_PO | | BCUSER |
| | | | CSMREG |
| | | | DDIC |
| | | | FDEVAUX |
| | | | RFCUSER |
| | | | RSHEFFER |

Sheet1

Ready

NUM



| | | | | |
|---|---|---|---|---|
| | | | TTEKLE | |
| | | | WEBLOGIN | |
| | | | WF-BATCH | |

vendor_master_create_and_PO_create_and_Goods_receipt

| Tcodes | Description | No_of_users_with_all_these_authorisation | Remarks |
|---|---|---|---|
| me21n | create_PO | | APAOLETT |
| mk01 | vendor_master_creation | | ARICHARD |
| migo | goods_receipt | | BATCH |
| | | | BCUSER |
| | | | CMCKEAN |
| | | | CSMREG |
| | | | DDIC |
| | | | DSCOTT |
| | | | FDEVAUX |
| | | | HBIJNI |
| | | | JGLEDHIL |
| | | 23 UESRS | JOUAREZK |
| | | | MDEBBAH |
| | | | NNOUAR |
| | | | PNG |
| | | | PSLESSOR |
| | | | RFCUSER |
| | | | RSHEFFER |
| | | | SAP* |
| | | | SMAHJOUR |
| | | | TTEKLE |
| | | | WEBLOGIN |
| | | | WF-BATCH |

6.5 The above screenshots show the list of users with different combination of duties set in accordance with the rules set by the auditor. The list was imported from Access to Excel. It could be seen from the above that there were 12 users who had access to almost all the functions of procurement, materials management and finance functions.

## 7. Audit Findings

***Segregation of duties analysis-Authorized users by transaction code***

7.1 It was noted that segregation of duties amongst SAP users dealing with various core functions like Budgeting, Procurement and Finance require a review by the Management as there were several users with access levels more than due for performing their day to day roles. Further, there were four users who had access to all the core Procurement and Finance functions like purchase creation, creation of Purchase Order, vendor master data creation, handling invoices/goods receipt and payment run. These were the users with SAP_ALL access, a privilege that gives the total access to the system which could lead to frauds. Two of them (includes the substitute) were dealing with only System Administration. Management was advised to review the matter.

7.2 In reply, the Management agreed that the matter merit further investigation in the coming months to determine whether the user list is valid or if action should be taken to further limit access to these transactions. Regarding SAP_ALL users, the Management while stating that the audit query raised was helpful in focusing their work on reviewing access and authorisations in the system, stated this issue had been recognised as an issue among

| | | | |
|---|---|---|---|
| | risk) | | |
| SA38 | ABAP/program execution | Execute ABAP programs | 10 |

7.8 While concurring with this observation, the Management replied that the users who have SE16, SA38 were from Finance and Publications Services and these roles are related to the DSA and Exchange Rate codes. It was assured to review and downsize the number of users, if need be, to only those that require these system transactions for their day to day work. It was also stated that there was a fundamental control in place over misuse of these transactions, namely that the Production system is locked for changes, with the exception of the time each month when uploads of DSA and exchange rates were being done and this had the effect of disabling these transactions except for the purposes of 'read only' and significantly mitigates the risk identified.

7.9 While appreciating the Management's commitment for preventing misuse of these transactions, in view of the observation on 'client 400-production under risk' (below) brought out in the report which identified that the production system remained open for changes, we recommend that the period for which the system is kept open for uploading the exchange rates be reviewed, besides reviewing the list of users with access to these transactions.

**Segregation of duties chart**

8.0 Based on the list of users with the conflicting duties that is vulnerable to fraud, a chart detailed below indicating the transaction code, number of users, risk associated with and suggestions, there of have been prepared.

**Conclusion**

9.0 In our opinion, though other internal controls are operating effectively, considering the number of users with super access and the list of users that were given the nature of access that is not required for their day to day working, there was a strong need for reviewing the access given. The above detailed approach of documenting the process and identifying the user-wise access and linking the users with super access enabled us in determining the vulnerability of the system to frauds.

the SAP user community in the UN system. It was further stated that UNICEF had reportedly arrived at a role which helped address the problem and they were in discussion with them to make use of their solution to improve their own control environment.

7.3 Audit recommend that the list of users with access to critical roles, including those with SAP_ALL be reviewed to restrict he access on 'need to know' or 'need to do' basis.

***Users with critical combination of duties***

7.4 There were 11 users (excluding SAP_ALL users) who could create a purchase order, create vendor master and receive goods receipt which are critical combination of duties in procurement function. Audit pointed out that for an effective segregation of duties amongst the users there was a need for reviewing this list for downsizing the same.

7.5 While explaining the compensating controls in place, the Management replied that the matter pointed out nevertheless merits further investigation and assured to take up the matter for improving the control environment.

***Users with critical budget functions***

7.6 According to the system requirement only two officers of the Management Accounting System wing deal with certain core functions of budgeting viz., Change plan values into original (CJ30) and Budget Release strategy (CJ32). It was however noted that there were 4 other users in the system that were not concerned with these functions but access to these transactions was given. Two of them were from the Member Audit State &Internal Over Sight (MAS&IOS).

It was replied that the issue pointed out merit attention and assured to downsize the list restricting the access to only those that perform these functions.

***Access to powerful system transactions in SAP***

7.7 SAP system has certain powerful system administration transactions, for example T_codes SE16, SA38 and SU12. Incorrect use of these transactions could result in loss of data integrity, confidentiality, and security or performance aspects. It was therefore essential that these transactions are granted only to those users on need ('to view' or 'to perform') basis.

Security review of the SAP system revealed that there were 10 users (excluding those with SAP_ALL) with access to SE16 and SA38 transactions as detailed below. Only SAP_ALL users had access to SU12. The users with access to these powerful transactions may be reviewed to restrict the access on need 'to view' or 'to perform' basis.

| **Transaction** | **Description/risk** | **What is possible with this transaction?** | **Number of users (excluding SAP_ALL)** |
|---|---|---|---|
| SE16 | Data browsing (Key Finance tables may be at | Direct reading and writing to SAP R/3 tables | 10 |

| Process | T_code | Description | Number of users | Risk | Suggestion |
|---|---|---|---|---|---|
| Budgeting | CJ30 | Change plan values into original | 6 | As per the system requirement, only two officers of Management Accounting System are allowed to have this access. Risk of unauthorised access | The list merits a review for down sizing |
| Budgeting | CJ32 | Budget release strategy | 6 | As per the system requirement, only two officers of Management Accounting System are allowed to have this access. Risk of unauthorised access | The list merits a review for down sizing |
| Treasury | F-13 | Reconciling bank statement (manual clearing) post with clearing | 29 | There is only one person that actually deals with this function. Others without a need may have access to perform this function. | May be restricted to that deal with this function. Others may be provided with another customised code. |
| Finance | FS01 | Creation of G/L master record | 20 | Reliability of the chart of accounts | Master database may be more centralised |
| Finance | F-02 | G/L account posting | 30 | Reliability of accounting may be affected | This access may be given to only those concerned with G/L posting |
| Finance | F-43 | Enter vendor invoice | 29 | Inaccuracies in accounting | Analyse whether all of them deal with vendor invoices |
| Finance | SA38 | Upload exchange rates | 35 | Inaccuracies in accounting | Restrict it only to those deal with it |
| Finance- AP | F-53 | Outgoing payments | 27 | - | The list merits a review for downsizing. |
| Finance-AP | F110 | Payment run | 27 | - | |
| Procurement | ME51N | Purchase requisition | 156 | - | - |
| | MK01 | Vendor Master data creation | 26 | Duplication in vendors master data; blocked vendors may continue to remain in the system | Master data management should be centralised and restricted to few only. |
| | XK02 | Change vendor | 123 | Duplication in vendors master data ; blocked vendors may continue to remain in the system | Master data management should be centralised and restricted to few only. |
| | ME29N | Release Purchase Order | 23 | Risk of unauthorised payments | Review the list and restrict on need basis |
| | FK01 | Create Purchase Order-Finance | 16 | | Review the list and restrict on need basis |
| | MIGO | Goods receipt | 218 | - | - |
| | MIRO | Vendor invoice | 29 | - | - |
| | | | | | |
| Budgeting | CJ30 | Change plan values into original | 6 | As per the system requirement, only two officers of Management Accounting System are allowed to have this access. | The list merits a review for down sizing |

| | | | | | |
|---|---|---|---|---|---|
| | | | | Risk of unauthorised access | |
| Budgeting | CJ32 | Budget release strategy | 6 | As per the system requirement, only two officers of Management Accounting System are allowed to have this access.<br>Risk of unauthorised access | The list merits a review for down sizing |
| Treasury | F-13 | Reconciling bank statement (manual clearing) post with clearing | 29 | There is only one person that actually deals with this function. Others without a need may have access to perform this function. | May be restricted to that deal with this function. Others may be provided with another customised code. |
| Finance | FS01 | Creation of G/L master record | 20 | Reliability of the chart of accounts | Master database may be more centralised |
| Finance | F-02 | G/L account posting | 30 | Reliability of accounting may be affected | This access may be given to only those concerned with G/L posting |
| Finance | F-43 | Enter vendor invoice | 29 | Inaccuracies in accounting | Analyse whether all of them deal with vendor invoices |
| Finance | SA38 | Upload exchange rates | 35 | Inaccuracies in accounting | Restrict it only to those deal with it |
| Finance- AP | F-53 | Outgoing payments | 27 | - | The list merits a review for downsizing. |
| Finance-AP | F110 | Payment run | 27 | - | |
| Procurement | ME51N | Purchase requisition | 156 | - | - |
| | MK01 | Vendor Master data creation | 26 | Duplication in vendors master data; blocked vendors may continue to remain in the system | Master data management should be centralised and restricted to few only. |
| | XK02 | Change vendor | 123 | Duplication in vendors master data ; blocked vendors may continue to remain in the system | Master data management should be centralised and restricted to few only. |
| | ME29N | Release Purchase Order | 23 | Risk of unauthorised payments | Review the list and restrict on need basis |
| | FK01 | Create Purchase Order-Finance | 16 | | Review the list and restrict on need basis |
| | MIGO | Goods receipt | 218 | - | - |
| | MIRO | Vendor invoice | 29 | - | - |

**********