CHAPTER: VI

GAIL (India) Limited

Financial Accounting module of SAP

Highlights

Credit management was not exercised properly in absence of credit master data for customers.

(Para 6.6.1.3 and 6.6.2.1)

Repetitive payments (upto 61 times) were made to vendors though these had been classified under One-time vendors.

(Para 6.6.3.2)

Defective customisation in respect of depreciation on assets resulted in incorrect depreciation.

(Para 6.6.3.3)

Imperfect user roles and authorisation resulted in users having access to critical combination of functions; system sensitive and irrelevant transactions.

(Para 6.6.5.1 and 6.6.5.2)

6.1 Introduction

GAIL (India) Limited (Company) was incorporated in 1984 as a principal gas transmission and marketing company of India and has since expanded its activities into exploration, production, processing, transmission, distribution and marketing of petrochemicals, Liquefied Petroleum Gas and telecommunications.

Computerisation in the Company began in 1986 with the installation of minicomputers and implementation of in-house developed Payroll and Financial Accounting Systems. The Company implemented SAP ERP solution in August 2005 at an estimated cost of Rs.55 crore.

The Company covered its entire business through nine integrated SAP Modules♣. The SAP R/3 release version 4.7C has been installed on Solaris 9 operating system and platform and Oracle is used as database management system.

6.2 Scope of audit

Audit reviewed the general ledger, accounts payable, accounts receivable and asset accounting in Finance and Controlling (FICO) module and e-Security issues. Audit examined the transactions, system reports♣ and SAP Tables at Infohub, Noida.

6.3 Objectives of audit

♣ ***Material Management, Sales & Distribution, Plant Maintenance, Project Systems, Finance & Controlling, Human Resource, Production Planning, Quality Management and Customers Relationship Management***

♣***System Reports: Standard SAP reports and Company's customised reports***

♦***Computer Aided Audit Techniques***

The main objectives of audit were:

(i) To assess whether the FICO Module of SAP was customised as per the Company's requirements.

(ii) To check the adequacy and completeness of mapping of the Company's transactions in FICO Module as per business and managerial requirements.

(iii) To ensure that the information/documents/reports generated through SAP were accurate to meet all managerial, customer and statutory requirements.

(iv) To ensure that the roles and authorisation were properly defined and duties were segregated rationally.

(v) To assess the adequacy of e-Security measures adopted by the Company.

6.4 Audit criteria

The audit criteria included:

(i) The Company's policies, manuals and managerial requirements;

(ii) Industry rules and procedures and Government guidelines;

(iii) The Company's user policy and job profiles of users; and

(iv) Best practices in IT development and implementation.

6.5 Audit methodology

Audit was conducted by adopting the following methodology:

(i) Discussion/correspondence with the Management; and

(ii) Data extraction using standard and customised SAP Reports and analysis thereof using CAATs♦.

6.6 Audit findings

FICO module of SAP handles all the financial transactions of the Company. This module is used for maintaining books of accounts, Asset management and preparation of final accounts including balance sheet, profit & loss accounts, *etc.* Test check of transactions, balances and reports revealed following observations on accounts receivables, accounts payable, general ledger accounting and asset management:

6.6.1 Input controls

Integrity of data in any system rests heavily on the controls over input. The objective of input controls is to ensure that the data received for processing are complete, not previously processed and entered without duplication. Weak input controls may increase the risk of entry of irrelevant, incomplete, duplicate and redundant data. Following are the observations regarding input controls:

6.6.1.2 Vendor master

The Company is maintaining vendor masters for its Material Management and accounts payables transactions. It is essential that one vendor should carry one vendor code. The

Company was maintaining 44039 vendor master records, review of which revealed the following:

(a) Purchase orders placed on vendors with incomplete details

There were 94 vendor records carrying only the name and city and no further information about their address, telephone *etc.* On 7 vendors out of these 94 vendors, 11 Purchase Orders (POs) worth Rs.119.41 crore were placed during the period July 2005 to November 2007.The management assured (December 2008) to take corrective action.

(b) Duplicate vendors

There were 161 vendors carrying 333 vendor codes. Out of these, POs (15 Nos.) aggregating Rs.8.03 lakh were placed on four vendors carrying eight vendor codes during February 2006 to April 2008.

The management assured (December 2008) to take corrective action.

6.6.1.3 Missing credit master data

The Company was maintaining credit data of its customers, which includes credit limit and actual credit extended there against. It was seen that the credit data was not available for 5188 customers out of 9839 customers. Out of the above, 797 customers were carrying outstanding balance of Rs.1302.37 crore ranging from Rs.4 to Rs.115.25 crore.

Thus, the system could not be used to exercise credit management.

The Management stated (December 2008) that the Credit & Risk Management has only been activated in SAP system for Petrochemical (PC) and Liquid Hydrocarbon (LHC) customers as per the business requirements. The reply is not acceptable as the Company has failed to use an available feature of the system and moreover customers other than PC and LHC are also having credit master data in contravention to the reply.

6.6.1.4 Multiple vendors with same bank account

It was seen that there were 76 vendor records attached with 37 bank accounts; indicating risks of irregular payments.

The Management stated (December 2008) that it had prepared an exception report to identify vendor records with similar bank records. The reply, however, is not acceptable as during the verification, it was found that 21 bank accounts were attached to 43 vendors, while the report only pointed out 6 accounts with 14 vendors.

6.6.1.5 Data entry in general ledger (GL) accounts

Incorrect posting in GL accounts

During test check of general ledger accounts, it was found that incorrect entries were also posted in general ledger accounts. It was seen that:

(i) In GL account 6115620-Water Charges Township, one entry valuing Rs.5.46 lakh related to Electricity bill of Vijaypur was posted;

(ii) In GL account 6112920–Salary–Casual Labour-India, one entry valuing Rs.1.95 lakh related to 'Expense for GM ED Directors' was posted;

(iii) In GL account 6199380-Other Exp- Bank Charges, one entry amounting to Rs.1.41 lakh pertaining to courier charges was debited; and

(iv) In GL account 6199010-Other Exp–Demurrage and wharfage charges, one entry amounting to Rs. 0.25 lakh pertaining to telegram expenses was posted.

Absence of input control and supervision to ensure recording of transactions in the intended accounts resulted in defective Management Information System (MIS) and incorrect expenditure details, at the same time defeating the purpose of having designated GL accounts.

The Management assured (December 2008) to take corrective action.

6.6.1.6 Non-use of narration field of transactions

The data fields enabling transactions in SAP also have a provision to capture narration relating to transactions. This helps in bringing more objectivity and clarity in GL accounts.

During review, it was observed that entries were posted without compulsorily capturing the narration, thus making it difficult to trace the objectivity of the transaction.

Lack of input control and supervision to ensure the capture of narration compulsorily and correctly resulted in incomplete recording of transaction details and incomplete MIS.

The Management stated (December 2008) that majority of the entries in the financial books are autoposting and accordingly the narration feature has not been mandatory. The reply is not acceptable as the use of the field can atleast be made mandatory for non-auto postings and the issue could be explored with SAP.

6.6.1.7 Assets carrying negative value

As per the general principles of asset accounting, assets should not carry negative balances, since that will turn them into liabilities rather then assets. During review of assets for the year 2008-09, it was found that two assets were carrying negative balance aggregating to Rs.2.40 lakh.

The absence of input control in the system to disallow negative posting of assets resulted in defective MIS and wrong asset accounting, which led to misrepresentation of assets in the financial statements of the Company.

The Management stated (December 2008) that the assets referred are assets under construction and hence are carrying negative balance. The reply is not acceptable since assets under construction could not be taken into books of accounts as “assets” and necessary corrective action is required.

6.6.2. Validation checks

Sound validation checks are vital to the integrity of any system. Placement of validation checks in the system ensures that the data received for processing are genuine, accurate and properly authorised. Lacking validation checks may increase the risk of entry of unauthorised, irrelevant, redundant data. Following are the observations regarding validation checks:

6.6.2.1 Credit extended beyond credit limit

A review of credit management data of customers was carried out and it was seen that the credit extended was not validated from the respective credit limit prescribed. As a result, 307 customers, for whom the credit limit was defined as zero, were extended credit of

Rs.308.06 crore. Further, three customers were extended credit of Rs.19.21 crore against a credit limit of Rs.9.83 crore.

Thus, the system could not be used for credit management to restrict the credit sales and rationalise Company's accounts receivables.

The Management stated (December 2008) that the Credit and Risk management has been activated for PC and LHC customers only as per the business requirements. The reply is not acceptable as the customers referred included customers from LPG (transmission) and natural gas business. Moreover, the credit limit defined in the system has not been used as a controlling measure to rationalise sales thereby defeating the purpose of defining a credit limit.

6.6.2.2 Wrong classification of assets

For classifying similar type of assets in one group, the concept of asset class is used in SAP. Depreciation rate is attached to asset class to charge the depreciation accordingly on each asset in that class.

During a test check of 9400 fixed assets in 'Corporate Services', it was observed that 156 assets like airconditioners and refrigerators, carrying a book balance of Rs.14.41 lakh were classified into the asset class relating to Furniture and Fixtures despite the fact that separate asset class for these existed.

Wrong classification of assets due to absence of validation checks and proper supervision, resulted in wrong calculation of depreciation and defective MIS.

The Management assured (December 2008) to take corrective action.

6.6.3 Inadequate customisation of the system

To reap full benefits of any ERP solution, it is necessary for the organisation to customise the software as per its requirements and take care of various industry specific, Government specific and law specific issues such as local taxes, financial statements, *etc.* A review of customisation of the FICO module was carried out and the customisation was found lacking to the following extent:

6.6.3.1 Payments trail in SAP

To facilitate a trail on payment cycle it is necessary that date of vendor invoice and date of receipt of invoice are captured in the system. It was observed that the system had not been customised to capture these dates.

The Company, however, has a Bill Watch System (BWS), an in-house developed application, in place which is integrated with SAP. This helps in tracking the bills by vendors and management and brings transparency in payment cycle. For this, it is required that whenever an invoice is received from vendor, it is to be entered in BWS, when the system allots a receipt number which can be used to track its status.

A test check of transactions valuing more than Rs.10 lakh revealed that during the years 2006-07 and 2007-08, 2827 payments aggregating Rs.14386.66 crore were made without using BWS. Even after excluding payments to Government Authorities and banks, there were 1285 payments aggregating to Rs.12516.09 crore without using BWS.

Lack of customisation to capture necessary details in respect of invoices and to allow processing of payments without BWS resulted in inability of the system to track the payments and bring about transparency in payment cycle.

The Management stated (December 2008) that it has created an exception report to monitor the payments not routed through BWS. The reply is not tenable as the issue observed allowing of processing of payments without using the BWS system.

6.6.3.2 Misuse of one-time vendor feature

One-time vendor code is used in SAP for those vendors to whom payment is expected to be made only once and the Company does not want to assign a permanent code to that vendor. The details regarding one-time vendors are entered in the system by users at the time of processing payment transaction.

During the review, it was noticed that 515 vendors were made payments for 2 to 61 times, despite these vendors having been categorised as 'One-time vendor'.

Due to lack of customisation to block repetitive payments to one-time vendors, possibility of misuse of one-time vendor code could not be ruled out.

The Management assured (December 2008) to restrict the use of one time vendor code for repetitive payments.

6.6.3.3 Defective customisation in respect of depreciation on assets

In SAP, the assets are assigned an asset class and requisite depreciation rate is attached to each asset class to calculate the depreciation as per the accounting policy of the Company and the Companies Act, 1956.

A review of fixed assets as on 31 March 2008 was carried out and it was found that assets were not charged depreciation as per the accounting policy of the Company, which specifies that assets costing upto Rs.5000 were depreciated fully during the year *i.e.* charged to revenue during the year of acquisition itself and no balance was carried forward to the financial statements of next year. Details are as under:

(i) Six hundred and twenty five assets aggregating to Rs.16.32 lakh were either not depreciated or were partially depreciated during the year 2007-08 despite their individual value being less than Rs.5000 thereby leaving undercharge of Rs.13.96 lakh on account of depreciation in contravention of the accounting policy of the Company;

(ii) Three assets acquired during the year 2006-07, valuing Rs.0.70 lakh; were attached to a depreciation chargeable asset class, but no depreciation was charged on them during the year; and

(iii) Thirty seven assets aggregating Rs.14.04 lakh, each valuing more than Rs.5000, were completely charged off during the year and were carrying no value at the end.

Deficiency in customisation to map the business rule in correctly charging depreciation resulted in inaccuracies in the financial statements of the Company and defective MIS.

The Management assured (December 2008) corrective actions in respect of point (i) and (iii) and stated in respect of point (ii) that the depreciation for the year 2006-07 for the referred asset had been charged through the system. The reply is not acceptable as the

observation is not concerned with charging of depreciation for the year 2006-07, but for the year 2007-08 as no deprecation had been charged for the year 2007-08.

6.6.4 Non-use of system

The Company levies liquidated damages (LD) for late/undelivered POs. The system is not used for calculation of LD for delayed supplies of materials and services.

It was observed that during the year 2007-08, the Company charged Rs.5.49 crore from vendors on account of LD, without calculating the same through system.

Due to non-use of system to calculate LD, the Company was not able to reap the benefits of the system fully and left the calculation at the discretion of users.

The Management accepted (December 2008) the non availability of such facility in the system and also stated that it was already explored with solution provider and was found not feasible. However, it is reiterated that necessary provision to charge LD through the system may be built in so as to minimise the human interventions.

6.6.5 e-Security

In SAP environment, it is of paramount importance that various physical as well as logical security layers are established to ensure integrity, correctness and sanctity of transactions and security of business information. In addition, emphasis should also be given to rationalisation of users' roles and authorisation and segregation of duties.

6.6.5.1 Segregation of duties

Before deciding about the user roles and authorisation, system administrator should follow the principles governing the segregation of duties:

(i) Users that authorise transactions should not enter them;

(ii) Users that maintain master records should not enter transactions; and

(iii) In accounts payable, separate users should maintain vendor master records, enter invoices and pay invoices.

During review it was noticed that segregation of duties among SAP users dealing with various core functions requires a detailed review by the Management.

(a) Users with critical combination of procurement functions

The major functions in a procurement cycle include placing of Purchase Requisition (PR), release *i.e.* approval of PR, creation of PO, release of PO indicating approval of the same, creation of vendor masters, modification in vendor masters, receive goods, receive invoice and process payments. Since, all these functions have a bearing on outflow of funds; the rationalisation of combination of transactions assigned to users was important.

During review it was found that users enjoyed various combinations of critical transactions, the details of which are as follows:

(i) Eight hundred users were authorised to create PR and release *i.e.* approve the PR;

(ii) Nineteen users were authorised to create PO and release *i.e.* approve the PO; and

(iii) Thirteen users were assigned roles to receive goods (Make Goods Receipt Voucher) and process vendor invoices.

The Management assured (December 2008) to review and rationalise user roles and authorisation.

(b) Users with critical combination of sales and distribution functions

The major functions in a sales and distribution module cycle include creation of customer master data, customer master data maintenance, creation of sales order, processing outbound deliveries, process sales invoices, maintain credit master data of customers**,** *etc.*

During review it was noticed that users were assigned critical combinations of transactions, the details are as follows:

(i) Two hundred and seventy three users were assigned authorisations to process sales orders and process outbound deliveries which had the risk of a user being able to create or change sales orders and deliveries to hide misappropriation of goods;

(ii) Two hundred and seventy six users were authorised to process outbound deliveries and process customer invoices which involved the risk of a user being able to create or change a delivery and create or change invoice;

(iii) One hundred and sixty users were assigned roles to maintain customer credit master data and incoming payments which involved the risk of a user being able to create a customer and then post payments against the customer;

(iv) One hundred and twenty seven users were assigned roles to maintain customer credit master data and process outbound deliveries which involved the risk of a user being able to create a customer and deliver goods to the customer and thereby misappropriate goods;

(v) One hundred and forty three users were authorised to process outbound deliveries and process incoming payments which involved the risk of a user being able to create incorrect or fictitious delivery and enter payments against these; and

(vi) One hundred and seventy eight users were authorised to process sales orders and process incoming payments which involved the risk of a user being able to create or change a sales order and process incoming payments inaccurately or fraudulently.

The Management assured (December 2008) to review and rationalise user roles and authorisation.

6.6.5.2 System administration

The authorisation to transactions should be monitored and rationalised by system administrators. Transactions attached to various SAP users and their respective job profiles were reviewed and following irregularities noticed:

(a) Authorisation of system sensitive transactions

There are certain system sensitive Transaction Codes[♣] (T-Codes) in SAP which are highly critical in nature *i.e.* the access to these T-codes should not be extended to users

[♣] ***Transaction Code: Used to identify various screens in SAP***

other than Superusers♦ and System Administrators, as it posed a risk to the smooth working of organisation.

Review revealed that users other than Superusers and System Administrators were also extended access of some system sensitive transactions like SE38, SA38, SE16, SM20, *etc.* This posed risks to the system like ability to perform development related functions; ability to run programs directly in the background; bypassing transaction level security; access to all the tables; access to all the sensitive data like personal details; and ability to view the security logs to name a few.

The Management assured (December 2008) to review and rationalise user roles and authorisation.

(b) Irrelevant authorisation

In a SAP environment, the users are given authorisations to execute transactions according to their profile to avoid undue load on the system and possibility of conflicting roles being attached to any user.

A review of the user profiles and roles attached revealed that common users were also extended authorisation to create or change PO; individual or collective release of PO; create goods receipt for invoice verification, *etc.* This posed the risk of user being able to carry out transactions that he was otherwise unauthorised to perform.

The Management assured (December 2008) to review and rationalise user roles and authorisation.

6.7 Conclusion

The absence of input controls and validation checks coupled with inadequate supervisory controls led to presence of unreliable data in the system. Inadequate customisation and mapping of business rules led to incomplete or incorrect capture of data apart from non-availability of important features for control on the purchase process and audit trails. Absence of adequate security through the role and authorisations and grant of authorisations to critical combinations and sensitive transactions made the system vulnerable to misuse and manipulation. Thus, not only was the system insecure, it was not appropriately customised and also contained unreliable data to be of effective use to the Company.

6.8 Recommendations

The Management may consider following measures to optimise the benefits from such an investment in the ERP system:

- Strengthening of input controls, validation controls and internal controls procedures to ensure accurate, reliable, pertinent and complete capture of data.
- Ensure customisation and usage of the ERP Solution as per business requirements, statutory requirements and guidelines of the Government and policies of the Company.

♦ ***Superuser: A special user who has privileges to perform all administrative tasks on the system. Superuser has the special powers like ability to read and write to any file, run all programs etc.***

- Proactively pursue with the solution provider to explore possibility of various scenarios such as calculations of LD, etc in the system.
- The 'Master Data' needs to be revisited/reviewed periodically for ensuring veracity of data and authorisation thereof.

The matter was reported to the Ministry in November 2008; reply was awaited (January 2009).