CHAPTER 3
MINISTRY OF SMALL SCALE INDUSTRIES

OFFICE OF THE DEVELOPMENT COMMISSIONER (SMALL SCALE INDUSTRIES)

Information Technology (IT) Audit of Small Enterprise Information & Resource Centre Network

Small Enterprise Information and Resource Centre Network (SENET) project was implemented by the Small Industry Development Organisation (SIDO) in 2002 as an e-governance project to provide an all India and decentralised information network for meeting the information requirements of small enterprises and other target groups. Major findings of the IT audit of this project are as follows:

HIGHLIGHTS

- **There was no policy for updating the information regularly on the website and the content regarding trade policy, clusters, state industrial policies, reservation policies, policies for small sector industries, annual reports and trainings was not being updated regularly.**

(Paragraph 3.4.1)

- **The SENET application did not provide for adequate input validation checks, which made the system prone to erroneous data entry resulting in unreliable information.**

(*Paragraph 3.4.2)*

- **There were significant deficiencies in the security of the IT system, covering restriction of unauthorized login attempts, review of logs, password policies, network security and logical access controls.**

(*Paragraph 3.4.5)*

- **SIDO was relying on external agencies for the management of the IT system, and had incurred an expenditure of Rs 183.65 lakh till March 2006, with a further commitment of Rs 39.80 lakh for the next two years.**

(Paragraph 3.4.3.1)

- **SIDO did not have a uniform policy regarding hosting of web sites and their maintenance by SISIs and a total expenditure of Rs 114.33 lakh was incurred on ISDN / leased line connectivity and web site hosting and maintenance by SISIs and reimbursed by**

SIDO during 2002-2006. Further, SIDO incurred an expenditure of Rs 48.99 lakh till 31 March 2006 on leased line connectivity for SIDO headquarters without conducting a formal technical feasibility study.

(Paragraph 3.4.3.2)

- **Neither internal audit nor any independent auditor was associated at any stage with the SENET project. There was no documentation evidencing the setting up of a quality assurance mechanism by SIDO. Further, there was no evidence of system testing for the applications implemented in SIDO, and the user and system documentation was inadequate.**

(Paragraph 3.4.4.1)

- **Only three modules – namely payroll, ISO 9000 reimbursement and entrepreneurial training – out of the 16 Office Automation (OA) modules were being used. Even in respect of these modules, SIDO was not relying on the electronic data and was still relying on the manual system.**

(Paragraph 3.4.6)

SUMMARY OF RECOMMENDATIONS

- **SIDO may take steps to ensure that the different Office Application (OA) modules are utilised and also that adequate input validation checks are built in to ensure correct and complete data so that the IT system can be relied upon instead of resorting to manual records.**

- **SIDO may ensure effective implementation of measures to ensure that the data on SIDO online is kept uptodate, and also monitor the website on a periodical schedule to ensure that old and outdated information is detected and updated.**

- **SIDO may formulate a uniform policy for web related services for all SISIs, as well as SIDO Headquarters and evaluate alternatives for choosing the most cost-effective solution meeting its requirements.**

- **SIDO may formulate and implement a formal IT security policy and detailed IT security procedures to ensure the confidentiality, integrity and availability of IT assets (including data).**

3.1 INTRODUCTION

The Office of the Development Commissioner (SSI), an attached office of the Ministry of Small Scale Industries, also known as Small Industry Development Organisation (SIDO), is an apex body for formulating and overseeing implementation of policies for the development of small scale industries in the country.

SIDO also:

- ∗ provides techno-economic and managerial consultancy;
- ∗ provides common facilities and extension services to small scale units;
- ∗ provides facilities for technology upgradation, modernisation, quality improvement and infrastructure;
- ∗ develops human resources through training and skill upgradation; and
- ∗ implements and monitors various schemes such as credit linked capital subsidy scheme for technology upgradation, credit guarantee scheme, ISO 9000/ISO 14001 certification reimbursement scheme, small industry cluster development programme, and assistance to entrepreneurship development institutes.

SIDO has a network of 30 small industries service institutes (SISIs), 28 branch SISIs, seven field testing stations (FTSs) and four regional testing centres (RTCs).

3.2 SENET Project

3.2.1 Overview

SIDO conceived (1993) and commenced (April 1997) with the approval of Standing Finance Committee of SIDO an e-governance project, Small Enterprise Information and Resource Centre Network (SENET) at a cost of Rs 4.35 crore. The project was modified in March 2000 and its scope was enlarged to include office automation applications and website at a project cost of Rs 11.40 crore.

The objectives of the project, as stated in April 1997 by SIDO, were:

- ∗ to provide an all India and decentralized information network, primarily for meeting the information requirement of small enterprises and other target groups such as the State Governments, directorate of industries, state industries development corporations, technology institutions, CSIR laboratories, industry associations and NGOs in their decision making process;
- ∗ to provide appropriate training inputs to the personnel in SIDO and its associate institutions; and
- ∗ to provide limited financial assistance to information agencies to implement information software packages.

The expanded project consisted of three applications viz., SENET Applications, Web Hosting, and Office Automation (OA) Applications. These applications were developed by CMC Ltd. and implemented during February 2002.

The network comprised of 31 electronic 'nodes', with the Main Node located at the headquarters of SIDO. Out of the 30 SISIs, 5 SISIs had Technology Nodal Centres[1] (TNCs) and 25 SISIs had User Centres (UCs)[2].

3.2.2 SENET Applications

SENET Applications provide a user interface to Main Centre (MC)/TNC/UCs for entering information on twenty six information categories, which is displayed on the web site to meet the requirements of entrepreneurs, SIDO and consumers. Some of the important modules are:

- ‘Product Profile’ module, which allows entrepreneurs to enter details of various SSI related products;
- ‘Project Profiles’ module, which contains the details of projects with regard to the product, financial outlay, production capacities and suppliers of raw materials /items profiles etc., which are prepared and updated by the technical officials of SIDO;
- Clusters[3] module, which provides information about the clusters and the small-scale enterprises comprising the clusters in India;
- Directories module, which provides names, addresses and other details of various organizations under SIDO and related to its business;
- Events module, which serves as a calendar for the various Training Programmes, Workshops and Awareness Programmes which are conducted by SIDO, or on which information may be available; and
- Yellow Pages, which provide individual firms a forum to advertise their business and marketing information.

3.2.3 Website

SIDO’s Internet website, also called SIDO Online, was set up for providing value added information to Indian small and medium enterprises (SMEs) and acting as a resource centre for bringing together diverse Small and Medium Enterprises (SME) related groups, entrepreneurs (existing and potential), associations, buyers, sellers, technocrats, training cells, technology developers and academia. It has been hosted on servers installed in the SIDO.

3.2.4 Office Automation Applications

These consisted of 16 Office Automation modules listed below:

[1] SISI Calcutta, Mumbai, Chennai, Bangalore and Ahmedabad

[2] SISI, New Delhi, Guwahati, Patna, Panjim, Solan, Jammu, Trichur, Indore, Cuttack, Ludhiana, Jaipur, Kanpur, Hyderabad, Karnal, Gangtok, Agartala, Agra, Allahabad, Muzaffarpur, Haldiwani, Ranchi, Hubli, Imphal, Nagpur, Raipur.

[3] A Cluster is generally identified by the product (or product range) and the place where it is located Examples of SSI Clusters in India are : Ceramic Pottery Cluster at Khurja, Leather & Leather Garments Cluster at Chennai, Hosiery Cluster at Calcutta etc

Personnel Information System; Payroll; Financial Accounting System; Budget; Parliament Questions; Audit Paras; Human Resource Management System; Entrepreneurial Training; General Administration; Publicity; Meetings (ISO 9000 reimbursement); Statistics of Small Scale Industries; Progress Monitoring; Diary Dispatch and File Tracking System; Complaints and Grievances System; and Court Cases System.

3.3 AUDIT SCOPE AND METHODOLOGY

An IT audit of SIDO covering the period from April 1997 to March 2006 was conducted from April 2006 to July 2006, using audit guidelines under the CobiT[4] framework. Data for the period April 2002 to March 2006 pertaining to SENET was analysed using Microsoft Access.

The draft report was issued to SIDO in September 2006, and an exit conference was held with the Development Commissioner (SSI) in October 2006. Responses from the Department were received in September and October 2006 which have been incorporated, as appropriate, in the report.

3.4 AUDIT FINDINGS

3.4.1 Invalid and Outdated Content on SIDO Online

There was no policy for updating the information regularly on the website to ensure timely dissemination of relevant information to the users which was the main objective of the project. Audit noted that the content regarding trade policy, clusters, state industrial policies, reservation policies, policies for small sector industries, annual reports and trainings was not being updated regularly. For example:

∗ The Trade Policy on the website referred to the previous EXIM policy 1997-2002, while the section on India’s Industrial Policies contained policies only upto July 1991. The section on SSI Policy Statements contained the Statement issued in August 1991.

∗ Information on participation in international trade fairs, exhibitions and training sessions pertained to the year 2000-01.

∗ While the “Know SSI” Version 3.0 CD had already been issued, the website gave details of the Version 2.0 CD.

∗ The data on handtools industry – import and export, export destinations, number of units and number of workers – pertained to the years from 2000-01 to 2002-03.

∗ Expenditure incurred on the ISO 9000 reimbursement scheme was available only upto March 2002.

[4] The Information Systems Audit and Control Foundation has developed standards known as CobiT (Control Objectives for Information and Related Technology). CobiT standards are tools generally applicable to, and are an accepted standard for IT governance.

∗ Information on technology requests and technology offers pertained to the period upto March 2001.

∗ The list of Annual Reports contained Annual Reports only upto 2002-03.

Audit also noted that the Application Server was found to be down frequently which restricted use of various web-based facilities. Also, a test of the website conducted on 30 June 2006 revealed that out of a total of 3068 hyperlinks[5] on the website, 42 hyperlinks were invalid.

In their response, SIDO stated as follows:

∗ In the course of Government business, there were requirements and demands from time to time about hosting websites for certain specific purposes within specified time schedules. Updating these websites on a regular basis was often not attended to with the same promptness with which they were created.

∗ The audit observations had been noted carefully and remedial action was being taken. All steps had been initiated to ensure that proper updating was done on a regular basis. The "MSMED Act, 2006" and "List of National Awardees" had been added to the website, while the web data pertaining to RTC division had been updated. The existing format of the Entrepreneurs Memorandum (in PDF[6] format) was under conversion into a writeable format for enabling online filing. Also, certain documents on the web were gradually being converted into downloadable format.

∗ A team of officers in SENET had been entrusted with the specific task of updating and monitoring the Web content regularly and continuously. Also, all the Divisions had been requested to go through the web content pertaining to their Divisions, and suggest modifications and deletions, if any, regularly to keep the content upto date.

Audit notes the action being taken by SIDO in response to its audit observations, and looks forward to full implementation of measures, whereby the data on SIDO online is continuously kept upto date.

Recommendation

SIDO may ensure effective implementation of measures to ensure that the data on SIDO online is kept upto date, and also monitor the website on a periodical schedule to ensure that old and outdated information is detected and updated.

[5] **Hyperlink,** also referred to as a link, automatically brings the referred information to the user when the navigation element is selected by the user. Combined with a data network and suitable access protocol, a computer can be instructed to fetch the resource referenced.

[6] **PDF – Portable Document Format**, an open file format created and controlled by Adobe Systems.

3.4.2 Weak Application Controls and Data Integrity for SENET Applications

Audit noted that the SENET application did not provide for adequate input validation checks. This made the system prone to erroneous data entry resulting in unreliable information as indicated below:

- The application accepted invalid characters (like *,#, %) in the data entry by users for division, designation, office type and office name, category of events, product codes, acknowledgement type and subject fields.

- SENET allowed fields like pin code, phone number, fax number, email address, details of turnover, registration numbers, registered office and details of quality certificates to accept blank or invalid characters and numerical fields to accept text also.

- Out of a total of 4351 records, blank data was found in:

  - 2211 cases in respect of name of contact person, phone, address, username and password

  - 245 cases in respect of pin code (in addition, 4 cases had text data);

  - 3763 cases, 3626 cases and 4351 cases in respect of turnover field, registration agency and registered office/ registration number respectively;

Further, in case of 4351 users, payment details of only 374 cases were available, indicating incomplete data entry. Also, control fields used by administrator for validation were all blank, signifying the fact that the information was being uploaded without any verification.

In response, SIDO offered no specific comments on the audit observations, but stated that the observations had been noted carefully and remedial action was being taken.

Recommendation

SIDO may ensure that adequate input validation controls are introduced in the SENET applicatio, to minimise entry of invalid data.

3.4.3 Ineffective Control over Operational Costs

3.4.3.1 Cost of Management of IT System

Audit examination revealed that SIDO was relying on external agencies for the management of the IT system and had incurred an expenditure of Rs 1.84 crore till March 2006 with a further commitment of Rs 39.80 lakh for the next two years, as indicated below:

- SIDO failed to develop its own team to take over the project after the extended support period for the completed project ended in September 2002. SIDO decided to outsource the maintenance of the project (facility management) to CMC at an annual cost of Rs 70 lakh on the basis of a single tender, without performing any benchmarking or study to judge the reasonableness of the cost of services. The contract with CMC was renewed for the year 2003-04 at a cost of Rs 69 lakh after inviting open tenders.

- Audit noted that the contract for the year 2004-05 was assigned to another firm for Rs 24.75 lakh (being the lowest bid); this contract was further extended for a period of 3 years at the rate of Rs 19.90 lakh per annum subject to satisfactory service.

Audit noted that SIDO had failed to train its own manpower, or consider the option of hiring NIC for maintenance of the system for cost effective maintenance..

In response, SIDO stated as follows:

- Under the agreement, the Annual Maintenance Contract (AMC) was to be given to CMC for at least two years. As SIDO staff had not been trained fully to take up maintenance work, the AMC was awarded to external agencies (as per the prescribed procedure).

- SIDO had since associated their own staff, and it was expected that they would be able take up the job of maintenance to a limited extent, after the existing AMC ended on 31st March 2008.

- After the completion of the existing AMC in March 2008, SIDO would consider NIC for further maintenance.

The reply of SIDO confirms the audit contention that the project planning and implementation were deficient as staff for maintenance job is still not equipped for maintenance a decade after its commencement.

3.4.3.2 Expenditure on Web Services

Audit noted that a total expenditure of Rs 1.14 crore was incurred on ISDN / leased line connectivity and web site hosting and maintenance by SISIs and reimbursed by SIDO during 2002-2006. Further, SIDO did not have a uniform policy regarding hosting of web sites and their maintenance by SISIs as depicted below:

- There was significant variation in expenditure incurred by SISIs on leased line connectivity and hosting and maintenance of websites.

- During 2004-05, four SISIs, namely, Goa, Gangtok, Agartala and Imphal tied up with NIC to avail the services free of cost.

- Thereafter, other SISIs were instructed by SIDO (August 2004) for exploring the possibility with their local state NIC authorities for hosting and maintenance of their web sites, however, without any positive outcome.

Further, SIDO incurred an expenditure of Rs 48.99 lakh till 31 March 2006 on leased line connectivity for SIDO headquarters without conducting a formal technical feasibility study. Audit noted that NIC had given (March 2004) details of available facilities for providing requisite connectivity.

However, SIDO outsourced the facility at a high cost and did not conduct a formal detailed technical feasibility study.

In response, SIDO stated that while allocating funds for web hosting and maintenance to SISIs during 2006-07, it had attempted to bring in a uniform policy to the extent possible, by advising SISIs to use the services of NIC wherever available. There was no response on the issue of leased line connectivity for SIDO headquarters.

Recommendation

SIDO may formulate a uniform policy for web related services for all SISIs as well as SIDO Headquarters and evaluate alternatives for choosing the most cost-effective solution meeting its requirements.

3.4.4 Other General IT Controls

3.4.4.1 Deficient IT Strategy

SIDO and National Informatics Centre (NIC) had jointly prepared a five year IT Plan (August 1998). Audit however noted that:

∗ The plan did not cover the field offices, i.e. SISIs, RTCs, FTIs and tool rooms. Also, although SENET was launched in April 1997, the Plan had only a brief description of SENET and did not include SENET's relation with existing or proposed databases and the role of SENET in overall IT effort of SIDO. Further, no time frame was set for realization of objectives.

∗ Neither internal audit nor any independent auditor was associated during the development, implementation, testing, monitoring and review of SENET. Association of these agencies would have helped in early detection of shortcomings.

While accepting the audit observations relating to internal audit/ independent auditor, SIDO stated that joint audit with NIC would be arranged for addressing the issues raised by audit.

SIDO also stated that due to financial and other administrative reasons, the Government decided to start the project with limited scope and develop it gradually.

3.4.4.2 Poor Project Monitoring and Quality Assurance

As per the revised SENET project approved in March 2000, two committees were to be formed for monitoring the project:

∗ a Project Implementation Committee (PIC) under the chairmanship of AS&DC (SSI), which was to ensure implementation of SENET in accordance with the approved milestones; and

∗ a Project Steering Committee (PSC) under the chairmanship of Secretary (SSI and ARI), which would review the implementation of SENET.

Audit noted that PIC met only twice during the implementation of the project, and there was no meeting held by PSC. Another committee – the

SENET Implementation Committee (SIC) was formed in June 2003 (i.e. after the implementation of SENET in February 2002) for supervising and guiding activities relating to the SENET project.

Further, as per the Detailed Project Report submitted by CMC:

- a quality assurance group was to be formed;
- project review teams were to be identified;
- peer level reviews and project status reviews were to be conducted at regular phases of the project life cycle; and
- standards for coding, documentation and error reporting were to be developed and followed.

However, audit could not find any documentation evidencing the setting up of such quality assurance mechanism.

In response, SIDO stated that they did not have IT trained staff when the project was taken up. It was for that reason that the competent authority preferred to engage CMC (a Public Sector Undertaking) to implement the project, and it was expected that CMC would take care of the quality assurance plan.

The reply is not tenable, as it was inappropriate to place complete reliance on the vendor responsible for the system design, development and implementation and expect that the vendor's own quality assurance mechanism would be adequate without a monitoring mechanism from SIDO's side.

3.4.4.3 System Testing

There was no evidence of system testing for all the applications implemented in SIDO. Only an Acceptance Test Plan (ATP) of the Office Automation modules, which was a mere description of the system, was available.

SIDO, in their reply (September 2006), stated that the observations of audit had been noted carefully and remedial action was being taken.

3.4.4.4 Lack of documentation

Audit examination revealed that:

- SIDO did not have a formal documentation policy.
- System design specifications and user manuals of SENET and OA Applications were not available.
- No documents relating to users' participation in development / implementation / testing of applications were available. Sign offs on completion of various modules were not obtained from actual users (to signify their acceptance of the completed modules).

In their response, SIDO did not offer any specific comments on the audit observations but stated that the observations of audit had been noted carefully and that remedial action was being taken.

3.4.4.5 Deficient Inventory Management

SIDO did not maintain an accurate record of its IT assets, as follows:

- ∗ SIDO did not maintain records of IT assets in various SISIs purchased for the SENET project in the following respects:
- ∗ SIDO could not provide a complete year-wise break up of expenditure under heads like AMC, leased lines, web site, computers, printers, networking equipment and software.

In response, SIDO stated that there may have been some inadequacies in maintaining the stock registers in respect of assets in SIDO Headquarters. However, the complete inventory had since been prepared, and the stock register and the head-wise expenditure registers were now being maintained.

3.4.5 Weak Security of IT system

Audit examination revealed significant deficiencies in the security of the IT system, as summarised below:

3.4.5.1 Restricting unauthorized login attempts

- ∗ No procedure to log unauthorized login attempts was in place.
- ∗ The application did not restrict the number of login attempts and the user id was not suspended after a specified number of attempts
- ∗ Concurrent sessions of the same user were not restricted.
- ∗ No advisory messages on log-on regarding list of successful/unsuccessful attempts, legal warnings etc. were available.

3.4.5.2 Logging

There was no formal system to review logs, in the absence of which, threats to system security would go undetected.

3.4.5.3 Password policy

- ∗ The passwords were not based on ‘single use authentication’, i.e., passwords were reusable, and the application did not enforce password change at specified intervals.
- ∗ SIDO did not have a policy of deactivation of former employee passwords.
- ∗ No formal system was in place for creating new users and passwords; and passwords were also being shared.

3.4.5.4 Security Policies and Procedures

∗ No written policy existed on downloading, acceptance, and use of freeware and shareware.

∗ Users had not received instructions on the detection and reporting of viruses, such as sluggish performance or mysterious growth of files.

∗ SIDO had not formulated a formal IT security policy and supporting procedures. No data classification schema was in place to ensure that all system resources had an owner responsible for security and content.

3.4.5.5 Network Security and Logical Access Controls

SIDO had selected (December 2002) the Centre for IT Security, CMC Limited, Hyderabad for conducting a security audit of the IT system. The report prepared (March 2003) brought out several weaknesses in the IT security set up of SENET like open ports, service packs/ patches/ hot fixes not installed on critical machines etc. As per the recommendations of the report, SIDO installed security devices like firewall and intrusion detection system at a cost of Rs 15.25 lakh. However, audit noted several weaknesses in the IT Security of SIDO, as detailed below:

∗ The traffic of SSI Network to internet was through a router[7], which had no logical security. As a result, Audit could easily access critical configuration details of the router and network from the router and was able to ping[8] the web server from the router. Similarly, the second router was also found accessible.

∗ The back up web server was remotely (logically) accessible with full access permissions from SIDO's intranet.

∗ Two switches[9] critical to the networking were accessible without any restriction which had the potential risk of making web servers, application servers and RDBMS server unavailable to users.

∗ The Oracle database server with default passwords and Norton Antivirus Server were accessible with full access permissions. Audit noted that various unnecessary programs were running on antivirus server which was very risky for the virus protection of entire network and web server.

Thus the setup contained significant vulnerabilities, potentially exploitable by a malicious user over the Internet.

[7] A **router** is a computer networking device that forwards data packets across a network toward their destinations, through a process known as routing. Routing occurs at layer 3 (the Network layer e.g. IP) of the OSI seven-layer protocol stack.

[8] **ping** is a computer network tool used to test whether a particular host is reachable across an IP network.

[9] A network **switch** is a computer networking device that connects network segments.

In response, SIDO stated as follows:

∗ The servers were installed in the SENET room in Nirman Bhawan, which was a highly protected area. Moreover, no case of exploitation by a malicious user over the internet had come to their notice.

∗ Though the IT security of the organization was not perfect, in a developmental organization like SIDO, there was hardly any closed information that required to be guarded. However, the organization would take abundant caution.

∗ SENET Division had installed an intrusion detection system to prevent unauthorized access to data.

The response of SIDO is not relevant as it does not cover the real issues as below:

∗ Physical security of the location is inadequate to prevent unauthorized access over the Internet or other networks.

∗ No data classification scheme was in place, which would enable identification of open and confidential/ secret information.

∗ The effectiveness of the intrusion detection system and other controls may be judged in the context of the security loopholes identified by audit.

∗ Information is not the only reason for attacks on networks. Various attacks result in defacement of websites, interruption in service, non availability of applications for data entry and reporting. Further, reinstating these services requires considerable time and cost.

Recommendation

SIDO may formulate and implement a formal IT security policy and detailed IT security procedures to ensure the confidentiality, integrity and availability of IT assets (including data).

3.4.6 Non-utilisation of Office Automation Applications

Even after implementation of the project in February 2002, only three modules -namely payroll, ISO 9000 reimbursement and entrepreneurial training - out of the 16 Office Automation (OA) modules were being used (September 2006). Even in respect of these three modules, audit analysis revealed that SIDO was not relying on the electronic data and was still relying on the manual system as described below:

3.4.6.1 Payroll

Crucial fields for generating monthly pay bills were not made mandatory e.g. basic pay, transport allowance, city compensatory allowance (CCA), dearness allowance (DA), dearness pay (DP), GPF contribution and pay bill number. Data analysis revealed that the database was deficient in the following respects:

- ∗ Out of 12159 records, there were blanks in 22 cases of Basic Pay, 57 cases of CCA, 101 cases of DA, 484 cases of provident fund number, 18 cases of DP and 18 cases of designation.
- ∗ DP was less than 50 per cent of basic pay in 42 cases and HRA was not equal to 30 per cent of Basic Pay plus DP (as required) in 41 cases.

3.4.6.2 ISO 9000 reimbursement scheme

Under the scheme, SIDO provides incentives to those small scale/ ancillary undertaking who have acquired ISO 9000/ISO 14001 certifications. An amount of Rs 48.53 crore was disbursed through this module during the period 2002-03 to 2005-06. Audit analysis of the database reflected duplicate certificate numbers in 137 out of 11519 cases of reimbursement against which approvals for making reimbursement was indicated, which the software/application was not able to detect. However, physical records did not reveal duplicate payment, which indicated that SIDO was relying on the manual records and not on the IT system before releasing the payments.

3.4.6.3 Entrepreneurial Training

The module is being used for storing information related to various training programmes organized by SIDO. Audit analysis, however, revealed following deficiencies in the database/application:

- ∗ In the table (3855 records) containing details of the entrepreneurial training course, the fields for name of the course and place of the course accepted blank or invalid characters.
- ∗ Fields like venue of training, and capacity of the course were not made mandatory, as audit noted blanks in 12 cases and 141 cases respectively.
- ∗ Details of expenditure and receipt realized in 243 cases and 1345 cases respectively were not entered in the database. As a result, generation of a report depicting correct status from the system was not possible.

In response, SIDO stated as follows:

- ∗ As per the objectives of Office Automation, it was intended to computerize the entire office, and hence 16 OA modules were got developed. However, due to non-availability of trained staff, only three out of 16 OA modules were being used.
- ∗ The remaining modules were being evaluated, and would be put to use in due course. Also, the existing staff would be got trained to use more OA modules. Further, they had requested NIC to study the existing infrastructure in SENET from the point of view of using available tools.
- ∗ The office had initiated the concept of network shared storage data, which would facilitate better server management, data management and data security.

The response of the Department is not tenable, as these factors – in particular, training and re-orientation of staff – should have been considered and planned before the implementation of the project. This is especially so, considering that SIDO took more than four years after conceiving the project to finally entrust the work to CMC.

Recommendation

SIDO may take steps to ensure that the different Office Application (OA) modules are utilised, and also that adequate input validation checks are built in to ensure correct and complete data, so that the IT system can be relied upon, instead of resorting to manual records.

3.5 CONCLUSION

Even after four years of implementation of the project, SIDO was not able to place reliance on the information being generated through the IT system and was relying on manual records. Network security was weak and SENET application did not provide adequate input validation checks. Office automation system was not implemented fully. Further, the information on the SIDO online was outdated and not being updated regularly. Thus, after incurring an expenditure of Rs 11.41 crore, the SENET project had not been able to fully achieve its objective of disseminating uptodate information in a timely manner to the small enterprises and other intended users.

(VIKRAM CHANDRA)
Director General of Audit
Posts and Telecommunications

New Delhi
Dated :

Countersigned

(VIJAYENDRA N. KAUL)
Comptroller and Auditor General of India

New Delhi
Dated :