

HOME (Police)/INFORMATION TECHNOLOGY AND COMMUNICATIONS DEPARTMENT

3.5 Information Technology Audit of eCops – an e-Governance initiative by Government

3.5.1 Introduction

Objective

The Director General and Inspector General of Police proposed (March 2000) to take up a comprehensive project of computerization of the Police Department at a cost of Rs 96.63 crore. This was with a view to build an improved information infrastructure to enhance the operational efficiency at all levels of the Police Department. The Project was to be implemented in phases; first phase was to cover all District Police Offices, all Police Training Colleges, all AP Special Police Battalions, and all Police Stations within the jurisdiction of three Commissionerates and Srikakulam District. In the second phase it was proposed to cover all other units and functional offices spread over the entire State. The online police network was to be implemented as a pilot project at the Commissionerates of Hyderabad, Vijayawada, Visakhapatnam cities and the district of Srikakulam covering a total of 279 units at an estimated cost of Rs 12.33 crore. Of these, Rs two crore were allocated for the development of software, Rs 6.73 crore were for the supply and maintenance of hardware and Rs 3.60 crore towards support services to be provided by the vendor.

3.5.2 eCops, an online policing e-Governance project

The Inspector General of Police (Computer Services) (IG) is in charge of the development, implementation and maintenance of eCops Project. In eCops package, the fundamental functional document called First Information Report (FIR), which records basic details of crime reported in any police station, gets registered by the computer system located at the police station and a unique FIR number in sequence along with system's timestamp is allotted to each crime reported; once registered and confirmed through the package the FIR can not be changed or deleted. The system facilitates registration of a crime at any police station or at a superior officers' computer, irrespective of jurisdiction limits and the same gets transferred automatically through this package to the relevant police station under whose jurisdiction the crime has to be registered and pursued. Information on crimes and criminals, missing vehicles and persons, current status of any FIR is provided to the citizen through web-enabled facility. The system encompasses all the existing investigation processes and

maintenance of all registers; besides generation of monthly crime statements and other MIS related reports.

Audit of the eCops project revealed certain deficiencies such as segregation of duties not made, inadequate access controls, inadequate user account and password management, lacuna in network infrastructure, inadequate application and data entry screen design, input validation, errors in data, implementation of back-up and recovery, inadequacies in database administration, integration and interfacing.

3.5.3 Staff not trained for System administration

There was no specific technical-staff hierarchy to cater to the needs of eCops Project. The department did not assess and identify the personnel required for the project clearly defining roles and responsibilities of each staff member. The IG stated that the police department entered into an agreement with CMC for rendering support services which includes imparting training to the selected police personnel on eCops usage and system administration. At the police station level only two personnel were trained to perform duties of data entry, day-end operations and taking data backup which is inadequate for round the clock operation. The department was totally dependant on CMC for Data Base Administration (DBA)/ System Administration activities, as the sanction for IT personnel was still pending with Government. There was no well-defined segregation of duties in respect of reconciliation, issue of access rights or exception reporting.

3.5.4 Inadequate access controls

Comprehensive security policy not implemented so far exposing the package to security risks

The data related to the hardcore criminals, extremist, anti-social elements was collected and stored on the computers for the use of police personnel. Thus adequate security policies and procedures should be drawn up and adopted to prevent data losses. However it was observed that comprehensive security policy was yet to be established and implemented in eCops. The operational users have access to tools like SQL plus which exposes database to unwanted elements, posing a serious threat to data security. The IG replied that access to SQL plus utility will be removed in future after complete stabilization of the system. The computer terminals were not located under suitable controlled facility, and since they store critical data, the access to the systems should be restricted to authorised persons only. In view of the sensitivity of the data and functionality, the department should have considered the option of implementing an exclusive security and access control software. Use of dial-up connections through modem in the project from police station to other systems enhances security risks. In the absence of any additional security measures for authorisation of user IDs (excepting oracle's default encryption), and application

authentication, security of eCops is in jeopardy. Besides, for most of the logins there were no corresponding logout recorded in the user log files indicating that application did not insist for proper logout. This would give scope for manipulation or misuse of data or database objects.

3.5.5 Inadequate user account and password management

Only one default application user widely used across all units despite the provision for creation of individual users

It was observed in audit that only one default application user was widely used across all the units within the department, despite the fact that the package provides for creation of individual users with definite roles and passwords. Default profiles created were used for all non-default users, which may give them scope to misuse privileges granted through default user profile. There was no well-defined password policy either for application, database or for operating system. It was observed that logical access controls were weak, exposing the system to serious risks of data manipulation. Password mechanism should provide for (i) changing the password by the users on their own before the expiry of a specified period; if this procedure is not followed, the system should not allow the user to perform his/her role (ii) automatic disconnect option if the user is not making use of the system continuously for a specified period of time. However no such controls were there in the system. Even the history of used passwords was not being maintained.

3.5.6 Lacuna in Network Infrastructure

Networking infrastructure is the lifeline of any modern IT infrastructure that is widely spread across many geographical locations. In rural areas the analog telephone systems used had snags which lead to failure of data transfer. The power transmission lines affected the telephone lines causing excess voltage at the routers and consequent damage. Since this was a recurring problem the department implemented a temporary solution by installing Analog RAS box, which is capable of withstanding excess voltage. The department in its reply stated that the BSNL authorities have been requested to maintain their telephone lines properly.

It was observed in audit that only the network-operating firm⁵² has control over network operations of eCops; and only selected few from AP police have been trained in Network Administration. There were no online monitoring tools on any system in the network or no mechanism existed to analyse protocols essential for ensuring network security. There were no specific network security measures adopted except for software firewalls and anti-virus gateways.

⁵² M/s Pioneer online private limited

3.5.7 Inadequate data entry screen design

Data entry screens did not provide for data flexibility

It was observed in audit that the data entry screens were not adequately designed to ensure capturing the essential data completely. The screens did not provide for flexibility for entering uncommon data. The system was also accepting technically or functionally non-feasible values in several input fields. The drop down list provided for certain fields contains irrelevant items. The search facility provided in some of the screens was not effective.

3.5.8 Effectiveness of the package

Except for registration of FIRs other important functional documents not maintained for many cases

The department had not conducted any evaluation of the effectiveness of the application through key parameters like response time, ease of interaction with system, completeness of the data, availability of information and help facilities. It was observed that in many cases except registration of FIR, other important documents like case diary, duty roster or chart, general diary, history sheets, rowdy sheets and suspect sheets were not maintained in system. Even daily status reports were not being generated through system. Though it was envisaged in the objectives of eCops that status of any FIR registered in any police station could be known through the Internet, this had not been implemented fully. Also most of the important fields were designed as non-mandatory; therefore the tables portrayed an incomplete picture. The very fact that 45 per cent of the transaction tables in the package and 58 per cent of the eCops related tables were with nil rows indicated that most of the functional data which is supposed to be captured into the package was not entered at all. The Consultancy firm observed that the potency of the package in supporting crucial functions was severely compromised due to reluctance of IOs and SHOs to readily supply information to update case records.

3.5.9 Input Validations

The input validations in the eCops package were inadequate. Some instances noticed in Audit are - there was no validation for checking the age input and the system was accepting occurrence time that is later than the time of FIR registration. The system accepted junk data in master tables, as well as in important fields. Though the system takes 'system date' as 'FIR date', there is a possibility of changing the system date and generating FIR for past or future date. The department in its reply stated that these would be attended to in the next version of the project.

3.5.10 Errors in data

There are FIRs without confirmation flags in the database although as per the business logic of eCops all FIRs should have confirmation flag. Non-confirmation of any FIR leaves scope for manipulating

them unauthorisedly as there was no specific trail on this information at any level. The Department replied that in the initial stages for building up acceptance of eCops by the users, relaxation in this matter was given. Facility was however provided in the software at DCP level for obtaining exception report of '*not confirmed FIR Nos*'. In the table containing terrorist description, there were non-terrorist items such as BJP, CPI and Bank officials. Out of 4014 records checked by Audit in the accused address details table, in 433 records the house number was left blank and in 752 records the house number values were duplicates or repetitions. In the table of accused details, out of 471 records checked the age was recorded as ZERO in 92 cases. In the table containing general diary of police station, it was found that there were more than 120 records out of 9996 records, which contained xxx as the entry in particulars column. The department replied that the errors pointed out would be rectified suitably in future versions.

3.5.11 Backup and recovery strategy planning and Implementation

The assets were not classified based on risk perception; in fact even the risk assessment itself was not properly done. Adequate alternative arrangements for continuing the activities in the absence of key personnel (both CMC as well as departmental personnel) for any reason were not in place. It was observed that backup was taken in the form of export files only and cold backup and OS backup was not taken at the police station. Testing of RAID technology implemented at Commissioner office/IG was not done periodically. There was no archive log at police station. Since databases at all the Police Stations were maintained only on single hard disks, the risk of losing important data looms was large. The recovery strategy did not comprise periodical test recoveries.

3.5.12 Shortcomings in log file management

No mechanism to backup the logs and document the 'rectification means'. The department is fully dependent on CMC for maintenance

Log files are very important to retrace the history of transactions. There was no documented procedure for maintenance of various log files and even for changes/modifications to the database. Though there was an inbuilt viewer utility for review of OS level log, no specific person had been identified to review these logs. Procedures of rectification measures were not documented. When this was pointed out the department replied that they have recently introduced the practice of maintaining the error logs on CDs. The responsibility of analysis of error logs was still with CMC and escalation of problems to the development team or support personnel was done by CMC only. There was no reporting mechanism to review the log files that monitor the activities of all the users. It was also observed that the system logs, database default logs and core dumps were not being resized from time to time both at

commissionerates as well as police stations. In the absence of such resizing activity at periodical intervals there was an imperative danger of database crash or even operating system crash.

3.5.13 Training

To familiarize the staff in operating the computer systems the department invited quotations to train police personnel, without explicitly mentioning any course requirements, on the plea that the project has to be rolled out by the stipulated date. During the course of training certain staff was withdrawn from training reportedly due to exigencies of work. After the basic training, the eCops end user training was imparted by CMC. The consultancy firm making cost benefit analysis observed that more than 55 per cent of PS officers did not even attend the two days eCops training in Hyderabad City. It was also observed that trained personnel were either transferred or diverted to other duties and untrained persons were posted to handle the computers. The consultancy firm also observed that about 30 per cent of those trained in Hyderabad were transferred to duties which did not involve the use of computers, such as traffic constables. Since the success of the package lies on the users, the functional officers should be periodically trained and the senior supervising officers should effectively monitor the training programmes.

3.5.14 Inadequacies in data base administration

There is a possibility to misuse the privileges granted through default user profile. No control to check and evaluate crucial database logs

It was observed that police stations, where functional data actually gets generated and stored did not have technically competent personnel to manage/administer the data. Though there were system Administrators trained to support police stations, their strength was inadequate to cater to the needs. It was observed that default database passwords for SYS and SYSTEM were not changed due to which databases were exposed to alteration and deletion by unauthorised persons. All data files including users and system table space files were located on the same Hard Disk. Also all copies of control files were located at same location in the same hard disk. There was no control in the system to check and evaluate crucial database logs such as alert logs and trace files of the database system; only application logs and network logs were periodically reviewed. It was also observed that database had many invalid objects; IG replied that these have since been rectified.

3.5.15 Lacuna in reports and forms

It was noticed by Audit that some of the queries provided in the package failed to show the required data in spite of the fact that qualifying rows existed in the database. When a particular FIR

number or name is entered, the details of the accused would not appear, as they should.

3.5.16 Conclusions

Audit of this e-Governance project to improve the efficiency and transparency in policing indicated mixed results in its implementation. The project suffered from serious security lapses, improper input validations, failure to elicit cooperation and acceptance at various levels. The plans of integrating and interfacing with all functionally related departments like hospitals; prosecution, judiciary and jails have not yet taken off. This falls significantly short of the objectives envisaged. eCops if implemented in its full form across the State has potential to improve the quality of policing significantly.

3.5.17 Recommendations

- Government needs to rectify the deficiencies so as to ensure that the outputs are accurate.
- Government should increase the efforts to make the project acceptable by the users by making functional heads responsible.

The above points were referred to Government in October 2004; reply had not been received (October 2004).