

PN-ACC-029



**STOCK HOLDING CORPORATION
OF INDIA LIMITED**
Review of Data Security and
Business Continuity Planning

**Financial Institutions Reform and
Expansion (FIRE) Project**

September 1996

**Financial Institutions Reform and Expansion (FIRE) Project
US Agency for International Development (USAID/India)
Contract # 386-0531-C-00-5010-00
Project #386-0531-3-30069**

**Price Waterhouse LLC
1616 North Fort Meyer Drive
Arlington, VA 22209
Tel (703) 741 1000
Fax (703) 741 1616**

Price Waterhouse LLP



September 12, 1996

Mr. R. Chandrasekharan
Managing Director
Stock Holding Corporation of India Ltd.
2nd Floor, Mittal Court
Nariman Point
Bombay - 400 021

Dear Mr. Chandrashekaran,

Re: Review of Data Security and Business Continuity Planning

As a part of our contract with USAID, we have completed our activity under Task Order No. 1. The purpose of this activity was to provide you with our comments, recommendations and insights as to the adequacy of your physical and data security surrounding, the processing of trade and related data as well as the adequacy of your business recovery plan.

Scope of Review

Our review included both **physical and data security** as it relates to the Pyramid Nile computers used for processing trades and back office functions at your installations at Nariman Point and Vikhroli.

Our review did not consider any aspects of your office automation systems in use.

More specifically, we reviewed the following platforms for adequacy of data security procedures:

UNIX
Relational Database System (ORACLE)

We also reviewed your overall **IS Security policies, physical security measures** and the **access controls** around the post trading and custody systems.

Since no efforts are to be put into developing a **business recovery plan**, we focussed our attention on how a plan should be constructed.



Our review has not included comments on the security of non-computer based paper documents. We suggest that this be taken up at the time of the detailed business continuity plan preparation effort, which would address this issue from the point of view of threats and countermeasures associated with such business resources.

Approach to Work

The security and business recovery aspects of this assignment were carried out by Price Waterhouse Senior Manager, Mr. Bimal Bhavanani, the lead Manager in our Information Systems Risk Management (ISRM) consulting practice in Bombay, aided by Mr. R. Raghu, Manager, and Ms. Pratima Dey, Officer.

Overall guidance for the work was provided by Mr. Walter D. Pugh, a retired Partner of the Price Waterhouse U.S. Firm with more than 35 years experience in all aspects of systems security.

Various work programmes that have been developed by Price Waterhouse firms on a worldwide basis were used both to guide us in our interviews with your staff and in reviewing appropriate documentation.

Findings and Conclusions

We must point out that this report is "**by exception**" and focuses on areas of residual risk and recommendations for risk reduction. Consequently, in this report we have not focussed on the controls which have been implemented. Notwithstanding these established controls, **there are areas of residual risk** which we believe are significant and need to be addressed on a timely basis.

In the changing environment of the financial markets, SCHIL needs to plan for the changes if it is to grow and become a more critical factor in the world financial markets. It is very important that you develop an infrastructure and **control environment** that is world class, i.e., processing is accomplished in a secure, timely and controlled manner, and, if there are problems, recovery is quick and mostly transparent to the users. This next step will require additional resources as well as a change in the control environment.



More specifically, our key findings on data security were that at the time of our review, **data security consciousness** was not as high as is needed in a world-class environment.

Although several of our recommendations have been implemented since the review was completed, these do not altogether remove the risk of unauthorized access to systems, particularly if there were to be some insider involvement. We identified a number of security features provided by the systems software components which had not been fully implemented as yet. Implementation of these could reduce the risk significantly.

We observed that management of data security was decentralized and different departments had initiated their own measures to ensure security. We believe that the absence of a centralized and independent data security. Our specific findings indicated that audit trails of security related events were not listed, and, therefore, not investigated.

Given that the security consciousness is not very high and that some security features of systems software have not been implemented, the risk of unauthorized activity on the system taking place and not being detected cannot be ruled out, in the absence of an independent security management function.

We therefore, **recommend setting up a security management function, raising the level of security consciousness and implementing the security features** provided by the systems software components. Guidance on implementing these recommendations has been provided in our detailed report.

In conclusion, we suggest that you implement our recommendations on logical security and physical security and also consider **encryption** of trade and other critical data.

At the time of our review, development of a Business Continuity Plan the planning process had yet to commence. The approach should be directed more towards ensuring continuity of critical business rather than just the recovery of computer systems. We believe that a business driven approach is required to ensure a comprehensive and practical plan. We recommend **appointing a project sponsor** (Managing Director or General Manager) and **a steering committee** comprising functional **heads**, as a number of business decisions are required for preparing a successful business continuity plan. To ensure an exhaustive plan, SCHIL also

September 12, 1996
Mr. R. Chandrasekaran
Managing Director
Page 4



requires a detailed **methodology** for business continuity planning, supported by **software tools** created for that purpose.

Next Steps

We suggest that we work with you under the **USAID FIRE Project** contract both to correct the weakness found and to develop the infrastructure to help prevent such weaknesses from surfacing in the future.

It is important that both steps be undertaken together. We have many findings and yet our review was not conducted in **great depth** in all areas. There are other weaknesses that have not been noted in this report. Similarly, if a more **control oriented infrastructure** is not developed, similar findings will occur in the future as systems develop further and new technologies are used.

The first step is for the management to make a commitment to establish such an infrastructure and control environment. Without the "**tone at the top**," further efforts are likely to be meaningful.

A **task force** should be established to fix the high and medium priority recommendation that we have included with this report. They should report to a high level within the Company.

In addition, a data security function should be established which, initially would include a data security officer and two support staff. This group should be charged with developing and implementing a well-controlled data and physical security environment. In addition, the development of the business recovery plan should be a part of their responsibility. They should report to a high level within the Company.

Pending USAID and SEBI approval under FIRE Project, we would be prepared to assist you in the above efforts by providing the following:

E



Proposed Areas for Further Work Under the FIRE Project

1. To evolve & prepare a Computer/Information Security Policy for SCHIL, including defining procedures, role & responsibilities of an Internal Systems Auditor etc.
2. To formulate Data Centre Operations Procedures/Policies.
3. To develop a Business Continuity Plan for SCHIL (technology & non-technology aspects).

As stated before, for this program to be a success, it requires encouragement and participation from the top management as well as a commitment of time and resources from your staff for these tasks to be accomplished. We can assist, but we cannot do the entire task.

Finally, we would like to express our appreciation to you and your other colleagues at SCHIL for the time, courtesy and cooperation extended to us during the study.

Please do not hesitate to contact **PW/FIRE Project, Mr. Bimal Bhavanani or me** at 494 6630/494 8718, 496 3599 or by fax at 496 3555, if you require any clarifications on this report.

Sincerely yours,

W. DENNIS GRUBB

PRINCIPAL CONSULTANT CAPITAL MARKETS

F

Stock Holding Corporation of India Ltd.

Review of Data Security and Business Continuity Planning

U.S. Agency for International Development
Price Waterhouse / FIRE Project

Mumbai
September, 1996

8

TABLE OF CONTENTS

1. INTRODUCTION.....	1
1.1 BACKGROUND.....	1
1.2 OBJECTIVES OF STUDY	2
1.3 SCOPE OF STUDY	2
1.4 PROJECT APPROACH.....	3
2. SUMMARISED TABLE OF RECOMMENDATIONS	4
3. DATA SECURITY REVIEW	8
3.1 SECURITY POLICIES AND MANAGEMENT	8
3.1.1 PURPOSE, OBJECTIVES, APPROACH AND OVERVIEW.....	8
3.1.2 RECOMMENDATIONS	10
3.2 SYSTEMS SECURITY	16
3.2.1 SOFTWARE SECURITY.....	16
3.3 PHYSICAL SECURITY AND GENERAL ACCESS CONTROLS	25
3.3.1 PURPOSE, OBJECTIVES, APPROACH AND OVERVIEW.....	25
3.3.2 RECOMMENDATIONS	27
4. SAFE CUSTODY SYSTEM (SCS) & POST TRADING SYSTEM(PTS).....	36
5. BUSINESS CONTINUITY PLANNING.....	39
5.1 PURPOSE, OBJECTIVES, APPROACH AND OVERVIEW	39
5.2 RECOMMENDATIONS	43
5.2.1 APPROACH TO BUSINESS CONTINUITY.....	43
5.2.2 CRITICAL EXPOSURES.....	46

1. INTRODUCTION

1.1 BACKGROUND

Stock Holding Corporation of India Limited (SHCIL) was established as a securities custodian and is presently the largest provider of custodial services in the country.

OBJECTIVES OF ENTERPRISE

- establish a nationwide facility for securities custody
- meet prevailing international standards

PRINCIPAL SERVICES

- Clearing House Operations (post trading, payment to/from clearing house, delivery and collection of securities, processing of transfers etc.)
- Safe custody of Securities (custody, deposits, withdrawals)
- Corporate action support (collection of dividend/interest, collection of bonus/rights securities, redemption/conversions, consolidation of securities, book closures, record dates etc.)
- Management information (reports related to various services mentioned above)

PROCESS CYCLE

The process cycle is divided into segments such as DIP (delivery instructions for purchase), Lodgements, Transfer Control, Databank, Objections, Safe Custody, Corporate actions, DIS (delivery instructions for sale), Reconciliations, Client Interface, Follow-ups and Safe Custody. Depending upon the volume, each segment is handled by several teams as may be required. Each team has to cater to a group of clients, for example, UTL, LIC, New India Assurance Company Limited, Morgan Stanley Growth Fund. Certain activities like data punching, bar-coding etc. have been outsourced to TCS (Tata Consultancy Services) and IIT services.

SYSTEMS SUPPORT

To facilitate the processing of transactions, various systems have been developed for SHCIL. PTS (Post Trading System) and SCS (Safe Custody System) were outsourced for development to TCS. These are operating under Oracle 7.0 on UNIX operating system. ABMS (Automated Bar-codes Management System) has been developed under Informix 5 on UNIX operating system.

SHCIL was nominated for **Smithsonian Award for the Year 1995 by Oracle Corporation** for extensive use of technology in its operations.

SHCIL Management has initiated this study with the goal to achieve higher standards and a more effective system of controls over its data and technology components.

1.2 OBJECTIVES OF STUDY

The objectives of this study were:

1. Review Data Security with specific reference to technology components
2. Review Business Continuity Planning

1.3 SCOPE OF STUDY

To accomplish the objective of this study, we reviewed the computing center environment, and the data security aspects of following applications :

- Post Trading System (PTS)
- Safe Custody System (SCS)
- Automated Bar-codes Management System (ABMS)

Data Security Review

The data security review focused on the implementation of technology components, including systems software, making up the Post Trading System, Safe Custody System and Automated Bar Code Management Systems. The physical security of systems and securities were also reviewed.

Business Continuity Planning

The Business Continuity Planning (BCP) phase was designed to provide recommendations for developing a business continuity plan (since there is no current plan that we could review). The BCP would formulate a course of action if there was a disaster to the operation of the business.

1.4 PROJECT APPROACH

We based our conclusions and recommendations on the basis of interviews with SHCIL personnel and documents provided by them.

Price Waterhouse methodology, which has been developed on a world-wide basis for use on similar reviews, was used for the review. As a result, our conclusions and recommendations reflect the combined experience from many such reviews.

The draft findings, implications and recommendations were reviewed by SHCIL management before being completed and submitted in this report.

The report has been divided in two sections, Data Security and Business Continuity Planning. The two sections are divided into subsections of related items. At the beginning of each sub-section there is a listing of the objectives, approach and objectives pertaining to that respective area. This is followed by the detailed recommendations.

We have summarised our recommendations and the level of priority assigned to each in the following section. We suggest that the high and medium priorities be implemented first, followed by implementation of the lower priority recommendations.

2. SUMMARISED TABLE OF RECOMMENDATIONS

REF NO	RECOMMENDATION	PRIORITY	MANAGEMENT COMMENTS
	SECURITY POLICIES AND MANAGEMENT		
3.1.2.1	DEVELOP AND IMPLEMENT A FORMAL SET OF DATA SECURITY POLICIES AND DETAILED PROCEDURES.	H	A
3.1.2.2	ESTABLISH A CENTRALISED DATA SECURITY FUNCTION.	H	P
3.1.2.3	STRENGTHEN CONTROLS OVER DIRECT FIXES TO THE DATABASE.	H	A
3.1.2.4	STRENGTHEN CONTROLS TO AVOID MISMATCH OF DATA IN PTS AND SCS DATABASE.	M	P
3.1.2.5	INITIATE STEPS TO ANALYSE DATA FIXES PERIODICALLY SO AS TO REDUCE THE NUMBER OF DATA FIXES.	M	A
3.1.2.6	ENSURE REVIEW OF DATA FIXES BY A SENIOR SYSTEMS DEPARTMENT PERSONNEL.	H	A
3.1.2.7	ENFORCE PROCEDURE FOR PASSWORD SELECTION AND CHANGE.	M	I
3.1.2.8	ESTABLISH PROCEDURES FOR GRANTING / REVOKING ACCESS TO USERS AND REGULARLY REVIEW THE ETC/PASSWD FILE.	M	I
3.1.2.9	STRENGTHEN PROGRAM CHANGE CONTROLS.	H	P
3.1.2.10	REVIEW SYSTEM LOGS.	M	A
3.1.2.11	ENSURE OFF-SITE STORAGE OF THE DATA BACKUP AND THE DATABASE CONFIGURATION PARAMETERS FOR SYSTEMS AT VIKHROLI.	H	I
	SYSTEMS SECURITY		
	SOFTWARE SECURITY - UNIX		
3.2.1.2.1.1	MAINTAIN AND REVIEW LOG OF PRIVILEGED USERS.	M	A
3.2.1.2.1.2	REVIEW HARDWARE VENDOR'S ROOT EQUIVALENT 'ICIM' USER-ID.	M	I
3.2.1.2.1.3	REVOKE ACCESS TO THE 'DBLINK' AND CONTROL 'FTP' USAGE OF THE APPLICATION DEVELOPMENT USERS.	H	P
3.2.1.2.1.4	REVIEW A LISTING OF FAILED LOGIN ATTEMPTS.	M	A
3.2.1.2.1.5	REVIEW DORMANT ACCOUNTS TO ENSURE THE NEED FOR THEIR EXISTENCE IN THE SYSTEM.	M	I

REF NO	RECOMMENDATION	PRIORITY	MANAGEMENT COMMENTS
3.2.1.2.1.6	ENABLE "AUDIT" OF OPERATING SYSTEM EVENTS. REVIEW AUDIT TRAILS GENERATED BY APPROPRIATE PERSONS.	H	A
	SOFTWARE SECURITY - ORACLE		
3.2.1.2.2.1	REVOKE DIRECT ACCESS TO THE DATABASE AND TABLES THROUGH SQL.	H	A
3.2.1.2.2.2	REVIEW EXECUTE PERMISSION GIVEN TO 'OTHERS' AND REVOKE WHERE NECESSARY FOR TOOLS SUCH AS SQLREP, SQLMENU AND SQLFORMS	M	P
3.2.1.2.2.3	MAINTAIN A SCHEDULE OF ACTIVITIES TO BE PERFORMED BY A DBA AND A LOG OF ACTIVITIES PERFORMED.	M	A
3.2.1.2.2.4	MONITOR THE ACTIVITIES PERFORMED BY USERS WITH DBA PRIVILEGES.	M	A
3.2.1.2.2.5	PROVIDE USERS WITH APPROPRIATE DATABASE ACCESS PRIVILEGES; REVOKE EXCESS ACCESS PRIVILEGES AT THE DATABASE LEVEL FOR EACH USER.	M	P
3.2.1.2.2.6	DEFINE AND ENFORCE THE CONCEPT OF REFERENTIAL INTEGRITY IN THE DATABASE THROUGH THE USE OF EITHER CONSTRAINTS OR TRIGGERS.	M	N. F.
3.2.1.2.2.7	DOCUMENT PROCEDURES FOR THE RECOVERY OF A DATABASE FILE USING A JOURNAL FILE; AND BACKUP JOURNAL FILES ON-LINE.	M	A
3.2.1.2.2.8	MAINTAIN ADEQUATE DOCUMENTATION OF ADDITIONS / CHANGES MADE TO THE METADATA DEFINITIONS.	M	I
	PHYSICAL SECURITY AND GENERAL CONTROLS		
	PHYSICAL ACCESS CONTROLS		
3.3.2.1.1	ISSUE GUIDELINES FOR KEY MANAGEMENT IN VAULTS AND ENSURE THEY ARE FOLLOWED	M	A
3.3.2.1.2	STRENGTHEN SECURITY MEASURES AT GULISTAN VAULT.	M	I
3.3.2.1.3	STRENGTHEN SECURITY MEASURES IN VIKHROLI VAULT AREA.	H	P
3.3.2.1.4	STRENGTHEN SECURITY OF THE COMPUTER SYSTEM CONTROLLING THE VAULTS.	H	A
3.3.2.1.5	RESTRICT ACCESS INSIDE VAULTS ONLY TO THE CUSTODY PERSONNEL.	M	A
3.3.2.1.6	AVOID STORAGE OF SECURITIES IN OPEN RACKS OR NON-FIRE PROOF CABINETS.	M	A
3.3.2.1.7	FORMALISE ACCESS AUTHORISATION	M	P

REF NO	RECOMMENDATION	PRIORITY	MANAGEMENT COMMENTS
	PROCEDURES AND RESTRICT VISITORS FROM SENSITIVE / VULNERABLE AREAS.		
3.3.2.1.8	POUCH LEVEL AUDITS SHOULD BE CONDUCTED AT MORE FREQUENT INTERVALS.	H	A
3.3.2.1.9	FORMALISE PROCEDURES TO RESTRICT ACCESS TO THE SENSITIVE SWIPE CARD ISSUING MACHINE KEPT IN THE CONTROL ROOM.	M	A
3.3.2.1.10	CENTRAL SECURITY ROOM SHOULD BE MANNED BY SECURITY AT ALL TIMES.	L	I
3.3.2.1.11	STRENGTHEN CONTROL OVER PHYSICAL MOVEMENT OF SECURITIES	M	A
3.3.2.1.12	DUPLICATE KEYS OF BINS OF GULISTAN VAULT SHOULD BE KEPT IN SAFE CUSTODY.	M	N. A.
3.3.2.1.13	SAFE KEEPING OF OBJECTIONS SECURITIES SHOULD BE STRENGTHENED.	M	A
	FIRE/FLOOD CONTROLS		
3.3.2.2.1	INSTALL FIRE/SMOKE/HEAT DETECTORS	M	A
3.3.2.2.2	REVIEW AND TEST ADEQUACY OF FIRE EXTINGUISHERS.	M	I
3.3.2.2.3	PRACTICE FIRE DRILLS AT ALL LOCATIONS.	M	I
3.3.2.2.4	TRAIN STAFF MEMBERS IN USAGE OF FIRE EXTINGUISHERS AT ALL LOCATIONS.	M	A
3.3.2.2.5	INITIATE STEPS TO ELIMINATE BREAK OF AN ELECTRICAL FIRE AT VIKHROLI.	M	I
	SAFE CUSTODY AND POST TRADING SYSTEMS		
4.2.1	STRENGTHEN CONTROLS OVER ACCESS TO THE APPLICATION SYSTEM BY USERS.	M	P, A
4.2.2	PROVIDE USER ACCESS TO THE PTS APPLICATION ONLY ON "NEED TO KNOW, NEED TO DO" BASIS.	M	P, A
4.2.3	DIFFERENTIATE MAKER AND AUTHORISER OF A TRANSACTION; PREFERABLY AUTHORISER SHOULD BE ONE LEVEL HIGHER.	M	I
4.2.4	ENFORCE ACCOUNTABILITY AMONGST VARIOUS "DIP" USERS.	M	A
4.2.5	OBTAIN DAILY REPORT OF CHEQUES RECEIVED AND HELD BY THE COLLECTION AGENT.	M	A
4.2.6	DEVELOP AND MAINTAIN ADEQUATE SYSTEMS AND OPERATIONS DOCUMENTATION.	M	A

REF NO	RECOMMENDATION	PRIORITY	MANAGEMENT COMMENTS
	BUSINESS CONTINUITY PLANNING		
	APPROACH		
5.2.1.1	ADDRESS BOTH COMPUTER DISASTER CONTINGENCY, MANUAL RECORDS AND INFORMATION TO ENSURE BUSINESS CONTINUITY.	H	A
5.2.1.2	CLARIFY PROJECT SPONSORSHIP AND OWNERSHIP AND DEFINE PROJECT MANAGEMENT ORGANISATION STRUCTURE AND PROCEDURES.	H	A
5.2.1.3	FOLLOW A DETAILED METHODOLOGY FOR BUSINESS CONTINUITY PLANNING.	M	A
5.2.1.4	ACQUIRE SOFTWARE TOOLS FOR BUSINESS CONTINUITY PLANNING.	M	A
	CRITICAL EXPOSURES		
5.2.2.1	ACTION CONTINGENCY PLANS FOR EQUIPMENT.	H	A
5.2.2.2	DOCUMENT TELECOM NETWORK.	M	A
5.2.2.3	BACKUP CRITICAL PAPER-BASED RECORDS.	M	A
5.2.2.4	SETUP COMMUNICATIONS WITH EMERGENCY SERVICES.	M	A
5.2.2.5	PLAN FOR SYSTEM FAILURES.	H	A
5.2.2.6	PLAN FOR POWER FAILURES.	M	A

PRIORITY

H - High

M - Medium

L - Low

MANAGEMENT COMMENTS

A - Accepted

I - Accepted and Implemented

P - Accepted but Partially implemented

N. F. - Not Feasible

N. A. - Not Applicable - Gulistan Vault is being closed down

3. DATA SECURITY REVIEW

3.1 SECURITY POLICIES AND MANAGEMENT

3.1.1 PURPOSE, OBJECTIVES, APPROACH AND OVERVIEW

Purpose

To ensure that management requirements for data security are clearly defined and implemented.

Objectives

- Confirm that responsibility for the management and administration of data security has been adequately defined to establish an overall control framework for the organisation with senior management support and commitment; and
- Identify areas of potential weakness or omissions in the security framework and management process.

Approach

Each of the areas shown below describes a set of control objectives that should be met.

- Security Policies and Standards should contain high level control objectives that define management's security requirements. These high level control objectives should include all aspects of security that could affect data confidentiality, integrity or availability.
- Detailed Personnel-Related Data Security Procedures should be prepared to include all security activities covered under the scope of the organisation's security policies and standards.
- The Organisation and Management of Security should include the allocation of responsibility for the management and administration of data security and for the ownership of systems and data. This would include technicians responsible for installing and maintaining security software, access control administrators, end users, developers and senior management.
- The Role of Internal Audit should include monitoring compliance with the organisation's security policies and standards and reporting any control weaknesses to management.

Overview

Procedures for the daily activities of the security management and administration functions should be defined and documented. The procedures should be designed to ensure full compliance with the high-level security objectives set out in the organisation's security policies and standards. The procedures should be detailed enough to ensure that individuals other than those normally employed in a given function would be able to take over in the event of an emergency. Care should be taken to ensure that the organisation does not place undue reliance on key individuals, particularly in the field of security.

Security measures should be implemented in a controlled manner and should be subject to independent review. Management should be aware of the security measures implemented and be provided with evidence that the level of security provided by a security measure meets the organisation's requirements.

Responsibilities for the management of data security should be defined, documented and allocated. Job descriptions of employees not directly responsible for security should define their individual responsibilities for data security given the scope and nature of their normal duties. These individuals should comply with the organisation's security policies and high level management control standards. Individuals with responsibility for security management or administration should not be assigned other responsibilities that could give rise to a conflict of security interest.

Reporting lines for individuals with responsibility for security management or administration should be either independent from the data function or at a senior level within the data function.

Responsibilities for the ownership of systems and data should be defined where the use of a centralised corporate database may hinder the task of identification of data owners. System owners should be designated.

Security measures should be used to enforce segregation of duties between incompatible functions. The minimum level of segregation of duties that should be achieved is the separation of the responsibilities for development, system support, change management, operations, user departments, internal/external audit and security management.

Individuals responsible for managing and administering security are often provided with privileges that could be used to gain unauthorised access to data. Another person should monitor and review these accesses.

3.1.2 RECOMMENDATIONS

3.1.2.1 Develop and implement a formal set of data security policies and detailed procedures.

A formal data security policy with detailed procedures does not exist. Security is largely dependent on the integrity of the individual personnel.

This may lead to a compromise of the security and control.

It is recommended that a data security policy statement supported by detailed procedures be developed and implemented. The statement should include policies on:

- the importance given to data security at SHCIL
- password secrecy protection, responsibility and access violation attempts
- emergency access procedures
- access profiles and segregation of duties
- backups
- virus protection

3.1.2.2 Establish a centralised data security function.

At the time of our review, data security was decentralized and embedded in other activities of each department.

As a result, the attitude towards data security and specific measures varied from department to department. Further, segregation of duties between users and data security personnel was not possible, as the persons who were vested with data security responsibilities were also responsible for carrying out other user functions. Such a structure has led to low priority being accorded to data security and ineffective surveillance. This could result in data security breaches and unauthorized activity on the system.

To overcome the risks while ensuring optimum utilisation of resources, it is recommended that a centralized data security function be established. The function could be headed by a **Chief Data Security Officer**, who should report to a high-level official (MD or Deputy MD). The function should be responsible for all aspects of data security and business continuity planning. Specific duties should include:

- Development and maintenance of data security policies and procedures;
- Creating awareness of data security in the organisation;

- Advising on controls and security in applications and physical security;
- Reviewing access rights regularly to ensure compliance with these standards;
- Identifying the owners of data entities to ensure maintenance of their integrity;
- Monitoring security and investigating security violation attempts;
- Reviewing security of existing data structures.
- Preparing, coordinating, testing and maintaining business continuity plans; and
- Providing training to personnel on data security, emergency procedures and business continuity plans

It is also recommended that the data security officers not be assigned any other functions on the system (including user administration). These officers should not be at a level below Manager.

3.1.2.3 Strengthen controls over direct fixes to the database.

Correction of the existing data is necessary in case of any discrepancy. For various operational and security reasons, modification permission is not given to the users. This correction is done by using a program SQLPLUS to get to the SQL prompt of the database and then manually correcting it (**Direct Data fix**).

When any person is allowed to do the data fix directly to the database without any audit trail, it is difficult to monitor the activities. Unauthorised modifications may accidentally or otherwise occur. This privilege to change or modify may be misused and may go undetected for an indeterminate period.

To overcome the risks, the following are recommended :

Remove SQLPLUS access with update, delete and drop privileges to LIVEDATA from all the users except two (one for the SCS and another for the PTS database). All others should be given only "select" privilege. Any change made to the database should be reviewed by a second individual.

3.1.2.4 Strengthen controls to avoid mismatch of data in PTS and SCS database.

The PTS and SCS database are inter-dependent and hence should be consistent at all times. But it is observed that the data fixes done in one database may not be updated in the other.

Inconsistency between PTS and SCS, could lead to confusion and wrong decisions. This would affect client service adversely.

A copy of updated data fix request forms should be interchanged daily between SCS and PTS personnel. They should verify the implication of each and every data fix carried out in the other database and update their database. This is necessary to ensure consistency between the two databases.

3.1.2.5 Initiate steps to analyse data fixes periodically so as to reduce the number of data fixes.

The data fixes carried out in PTS and SCS are filed without any regular review or analysis to find out if there are any recurring data fixes.

The number of data fixes should be reduced. Based on our limited review, the data fixes could number between 200 to 250 per month. The data fixes of this magnitude may be due to the inability of applications systems to take care of modification needs due to business and operational reasons. Management should be aware of the types of direct data fixes that are being done, so as to initiate action to reduce them.

The data fixes done at PTS and SCS should be analysed by the authorised personnel who are doing the data fixes. The software vendor should be consulted to provide the relevant programs to update for repeated data fixes. This analysis and its conclusions should be submitted to management every month.

3.1.2.6 Ensure review of data fixes by a senior systems department personnel.

At present, the data fix is initiated by the Deputy Manager or the Manager of the department which requests the data fix. The same is then reviewed by Manager of the Accounts department to determine whether the data fix will have any direct and immediate financial implication.

Any data fix should be approved by senior Systems Department person not less than the level of Assistant Vice President. The authorising senior person should understand all ramifications of the data fix requested and only then approve or reject the same. All data fixes done should be properly documented.

3.1.2.7 Enforce procedure for password selection and change.

At the time of our review, we observed that the general consciousness on the need for ensuring password secrecy was low. In case an employee goes on leave for a period of less than six weeks, his/her password is not locked.

This could lead to passwords for sensitive functions being used for unauthorized activity.

It is recommended that :

1. All users be educated about the criticality of maintaining password secrecy and password selection norms. Passwords need to be locked when an employee goes on leave.
2. The users be properly advised against selecting insecure passwords such as those with strong personal association or work-related terms. Mixed strings or nonsense syllables are preferable. The need to have such unrelated passwords should be explained to the users and they should be advised to have password with minimum length of six characters, at least with one numeric character to make it difficult for any unauthorised user to guess and break the password.
3. All application software should ensure that the password is not stored in clear text form to prevent misuse and compromise security.

3.1.2.8 Establish procedures for granting / revoking access to users and regularly review the etc/passwd file.

The system administration group is responsible for the creation and maintenance of the user-ids and their access profiles (as authorised by the user departments) in the system. The user departments are not reviewing the newly created user-ids. Also, the etc/passwd file that contains the home directories for all users alongwith passwords, is not being reviewed regularly by the systems department. It was observed that the etc/passwd file contained some dormant user-ids.

Under the circumstances, it is possible for unauthorised user-ids to be created; and also, authorised user-ids to be granted excessive privileges.

By verifying the user-ids and their privileges with their request form, creation of unauthorised user-ids / authorised user-ids with unauthorised privileges should be restricted. It is recommended that:

- procedures for granting / revoking access to the users be clearly defined;
- the user-ids / access profiles be reviewed by the user department head regularly;
- the etc/passwd file be reviewed by the systems department;
- dormant accounts be removed from the system.

The HRD / Personnel Department should provide the systems department with the names of people who are currently employed with the company. This should be reviewed and matched with the user profile table to ensure that user-ids of people not still employed with the company are deleted.

3.1.2.9 Strengthen program change controls.

Besides the executable files, the source code of the programs are also present on the production system and available to many different individuals. Consequently, changes to the program files are made directly on the production system.

Unauthorised changes to programs may be made, and consequently the programs may not be subject to adequate testing prior to implementation. This may lead to compromising data integrity; and also, documentation of changes made may not be kept up-to-date.

The source code should be maintained in a restricted area of the development machine program library and available only to limited number of individuals. Access to the program may then be granted to the programmer subject to the satisfaction of criteria required. This will also help ensure that the same program is not being modified simultaneously by two different programmers. After completion of the changes, the programs should be subject to exhaustive testing. Not only the programs that are changed, but also modules interfacing with the changed programs should be tested to ensure that there is no other impact of the changes. After obtaining approval from the end-user, the executable files may then be transferred by the authorised automation person to the production systems, the programs to the program library after assigning a version number to the system. The documentation pertaining to the changes should be updated at the same time.

3.1.2.10 Review system logs.

The system generates logs such as "sulog", the sysadm.log (System Admin Log) and the system performance logs.

These logs provide vital information about access violations and system performance. If these logs are not reviewed, timely corrective actions in case of system failure / crash may not be initiated.

These logs should be reviewed periodically.

3.1.2.11 Ensure off-site storage of the data backup and the database configuration parameters for systems at Vikhroli.

At present, the backup of data and database configuration parameters of systems at Vikhroli and those of Mittal Court are stored in fire-proof cabinets within the premises; however, no backups of Vikhroli are stored off-site.

In the event of a disaster, it may not be possible to recover data.

The backup of data and their parameters for Vikhroli operations should be stored off-site.

3.2 SYSTEMS SECURITY

Effective systems security measures help prevent unauthorised access to any kind of sensitive information. They also help protect equipment, software and data files from damage by tampering.

On any system there are two types of users: authorised and unauthorised. An authorised person has right to access the system and its resources according to the authorisation criteria set up by the system administrator. Unauthorised users have no right at all or have a restricted access either by time or resource.

Security breaches usually results from either:

- User irresponsibility - purposely or accidentally
- User probing - academic exploitation of insufficiently protected areas
- User penetration - skilled and malicious
- Social engineering - deception by intruder e.g. impersonation of users, operators etc.

The scope of the review was not to assess whether security breaches had occurred or not but to highlight areas where weakness' exist and provide our recommendations for these.

3.2.1 SOFTWARE SECURITY

3.2.1.1 Purpose, Objectives, Approach and Overview

Purpose

To evaluate the security functions relating to the installation, administration and use of software.

Objectives

- Confirm that adequate security functionality has been implemented within the software;
- Identify areas of potential weakness or omissions in the security functionality; and
- Recommend solutions to remedy identified weaknesses and omissions.

Approach

Each of the following scope areas shown below describes a set of control objectives which were to be met.

- Controls over User Identification and Authentication should include the mechanisms to establish a user's identity and to authenticate that identity. These include the use of electronic swipe cards as well as the more traditional user ID and password.
- Resources Profiles which are the translation of security requirements over resources such as data files and programs into access control rules should be appropriate to enforce the segregation of duties.
- Security Audit Trails which establish accountability for activities which have occurred and store violation information should be reviewed and actioned.
- Systems Software Administration which addresses the ongoing monitoring and operation of the systems software should be adequate to provide a safe environment.

Overview

Systems software provides the environment and platform for running the application systems. Systems software can comprise numerous sub-systems or modules which perform specific tasks (e.g., on-line editors, performance managers, security software). However, the overall security requirements for these various components is similar.

Each of the software components must provide the five core security functions:

- to identify and authenticate potential users of the system;
- to identify and record access rights to the resources of the system;
- to assess the access rights of the users to the resources and to react appropriately;
- to record security activities; and
- to maintain security information relating to the users, resources and security logs.

Each type of software service provided (e.g., operating system, database, telecommunications, security and operations) must provide a secure and controlled processing environment by implementing the above security functions. Where the individual software component does not provide this service, it must link (in a secured manner) to another software component so that, in totality, an adequate level of security is maintained.

In addition to the five core software security requirements, there are additional security requirements which should be addressed during a review of certain types of specific software components such as database systems. For example, database systems should

be expected to have a system of internal integrity checking (e.g., referential integrity for relational databases) to ensure the consistency of the internal data structure. To ensure that the base requirements as well as any specific requirements have been met, the review of software security should initially identify the various software components to be reviewed.

The requirements of the five core software security functions were reviewed and evaluated. Then, additional security functionality needed for the specific environment under review was addressed and included as appropriate.

3.2.1.2 Recommendations

3.2.1.2.1 Operating System - UNIX Rel 5 Ver 4

3.2.1.2.1.1 Maintain and review log of privileged users.

A user who has the 'root' privilege is the most powerful user in the UNIX operating system. There are several users on the system who are granted the 'root' privileges (such as those belonging to the systems administration group). Also, these users share the Database Administrator's (DBA) password. However, activities performed by these users are not being monitored. In addition, the external vendor (TCS) also has access to these privileges.

As these are privileged users, access to sensitive files through these user-ids is possible. Under the circumstances, it is not possible to maintain individual accountability for actions of such users.

It is recommended, that a manual log should be maintained which should contain details such as **name** of the user, the **time** of usage, the **reason** for usage and the name of the individual who has **authorised** the usage of the privilege user-ids. The manual log will help the management to have better control over the usage of these privileged user-ids and help fix accountability in case of any problem.

3.2.1.2.1.2 Review hardware vendor's root equivalent 'ICIM' user-id.

At the time of our review, the Hardware Vendor (ICIM) had a separate user-id 'ICIM' to carry out maintenance work. This password is a 'root' equivalent. It was noted in the 'sulog' (Set User Log) that other users, such as 'Hemant' were also using the 'ICIM' user-id.

It is difficult to control many privileged user-ids.

The systems department should review the need for the hardware vendor to have a separate 'root' equivalent user-id. If the access is allowed then the user-id should be monitored and the evidence of this monitoring should be available.

3.2.1.2.1.3 Revoke access to the 'DBLINK' and control 'FTP' usage of the application development users.

Separate machines are maintained for the development (SUN) and production (NILE) systems. However, the development team (vendor) is given access to the "DBLINK" facility to download production data from the NILE system to the SUN system for the purpose of testing the application software at the Mittal Court location. Also, the programs are moved from the development machine to the production machine by the developers through the 'FTP' facility.

Access to the live data by a vendor, should he be able to upload from the SUN to NILE systems may expose data to manipulation. Without adequate control over the access to the FTP utility, users would be able to navigate other directories and make changes to data / programs without authorisation; this may compromise the security of files in the system.

Usage of the FTP utility should be strictly controlled and monitored. The DBLINK facility to the production data may not be desirable. Only old data should be given for testing. The developer should not be allowed to access the production machine.

3.2.1.2.1.4 Review a listing of failed login attempts.

At the time of our review, there were many users on the system with failed login attempts.

Although, details pertaining to failed login attempts are being logged; reports of these failures are not being prepared.

Failed login attempts may imply unauthorised access attempts to valid user accounts.

A listing of failed login attempts should be generated periodically. These should be reviewed by appropriate officials.

3.2.1.2.1.5 Review Dormant accounts to ensure the need for their existence in the system.

There are many users in the system who have not logged in for more than 3 months.

Misuse of dormant user-ids is possible, should the password of the dormant user-id be available to any other individual.

It is recommended that a listing of dormant accounts (not used for more than 3 months) should be generated and reviewed periodically by appropriate officials to determine whether they should be removed from the system.

3.2.1.2.1.6 Enable "Audit" of Operating System events. Review audit trails generated by appropriate persons.

The 'audit' option of the Operating System has not been enabled.

When enabled, all activities of all users are logged for subsequent review. If there is a concern about degradation of performance, then the audit option can be enabled for only specific events. Otherwise, the management would not be able to monitor the activities of any of the users.

Audit option of the Operating System should be enabled for those events considered critical by management. A suggestive list of commands for which audit can be enabled is given below.

reboot , fastboot, shutdown, rename, halt, mount, unmount, open, close, chown, chmod, kill, rmdir, exit, fsck, sam or sysadm, bind, rm, su.

The audit trail generated should be reviewed by the appropriate person.

3.2.1.2.2 Database - Oracle 7.0

3.2.1.2.2.1 Revoke direct access to the database and tables through SQL.

The database / table 'modify' privilege is granted to the Data Base Administrators. Changes to structure of the tables are made by the DBAs. It is possible that :

- Unauthorised / invalid changes may be made to the data in the tables.
- Sensitive information might be deleted by mistake.

This could result in the loss of image in the market as well as monetary loss to SHCIL.

The users should not be given direct access to the database (and other related elements such as tables, constraints etc.) through SQL. The changes made should be examined and reduced.

3.2.1.2.2 Review execute permission given to 'others' and revoke where necessary for tools such as SQLREP, SQLMENU and SQLFORMS

The tools mentioned above facilitate direct access to the database. SQLREP, SQLMENU and SQLFORMS are tools used in development environments and have equivalents in the production environment with "execute" permission for others.

The implication is that any user at the Operating System level could use these tools to access the database and perform unauthorised activities.

It is recommended that the "execute" permission for users other than those who require to use these tools, be revoked from critical ORACLE tools on the production system.

3.2.1.2.3 Maintain a schedule of activities to be performed by a DBA and a log of activities performed.

A DBA performs the important task of maintaining a database which is being concurrently accessed by many users for different purposes. Consequently, it becomes very important to set high standards for maintaining the database in terms of security, consistency, reliability, integrity, accuracy, completeness, access speed / retrieval etc.

At present, there is no specific schedule developed for the maintenance of the database. Certain important functions such as 'Verifying' a database (to ensure that the database is not corrupt), 'Monitoring' of database characteristics, review of security audit log for unauthorised database access do not appear to be frequently carried out.

Improper maintenance of the database could lead to database corruption and loss of data integrity. This could go unnoticed and when noticed, it may be too late to recover.

To ensure high standards of database maintenance, a schedule of tasks to be performed by a DBA should be developed. A log of jobs performed vis-à-vis the schedule should be maintained to ensure that the standards are met.

3.2.1.2.4 Monitor the activities performed by users with DBA privileges.

A Database Administrator has certain privileged access rights which are required for the maintenance of the database. However, it should be ensured that these privileges are not misused.

As the role played by a DBA is very important to the business, it is very important to monitor the same, as some activities could be performed in an **authorised** manner and would go unnoticed.

Activities performed by a DBA should be monitored by an independent person with the help of the audit-trails generated by the RDBMS.

3.2.1.2.2.5 Provide users with appropriate database access privileges; revoke excess access privileges at the Database level for each user.

All "SCSAUTO", users (approximately 15) have access to modify objects; although all of them are not required to have the update and modify privilege. Since "SCS" is used as a generic login all those who login as "SCSAUTO" these users also inherit all the privileges assigned to it.

Giving access with single generic login will make it difficult to fix accountability.

Access privileges should not be granted in excess of "the need to know and need to do basis", as unauthorised activities may be performed inadvertently or otherwise. This can be controlled by defining individual users to the DBMS and giving access according to the individual need.

3.2.1.2.2.6 Define and enforce the concept of Referential Integrity in the database through the use of either Constraints or Triggers.

Referential integrity refers to the consistency of related pieces of information across multiple tables in a database. A column in a table can be defined as "referencing" a column in another table; such a definition establishes a constraint that prevents deletion of a row that has rows in another table dependent upon it, or from adding or modifying rows without a corresponding matching row in another table. At present, the concept of referential integrity is not used across all applications since they were upgraded.

Deletion of records in the master data file where records exist in the transaction data file would be possible without Referential Integrity being defined and enforced.

The concept of Referential Integrity should be defined and enforced in the database through the use of either Constraints or Triggers.

3.2.1.2.2.7 Document procedures for the recovery of a database file using a journal file; and backup journal files on-line.

Journal files are used to recover the database to a consistent state after a database crash. At present, there are no procedures defined and documented giving details as to how a database should be recovered using a journal file.

In the event of a database crash, it may not be possible to recover the database as the procedures for recovery are not clearly known or documented, and it may take undue time to recover the database. If the database and the journal files were to be lost simultaneously (e.g. in the event of disaster), it may not be possible to recover the database as the on-line backup of journal files has not been enabled.

The procedures involved in the recovery of a database file using a journal file should be documented and the on-line backup of journal files should be enabled.

3.2.1.2.2.8 Maintain adequate documentation of additions / changes made to the metadata definitions.

A file for request of changes from SHCIL users is maintained by the DBA. However, documentation of the changes made to metadata definitions is not updated.

Consequently, details pertaining to changes made is not readily available. As a result there is a greater dependence on an individuals' knowledge which impacts the Data Administration group.

Adequate documentation on additions / changes made to the metadata definitions should be maintained.

3.3 PHYSICAL SECURITY AND GENERAL ACCESS CONTROLS

3.3.1 PURPOSE, OBJECTIVES, APPROACH AND OVERVIEW

Purpose

To assess the adequacy of physical security protection within the overall IS environment and for securities handled.

Objectives

- Conclude on the overall adequacy of physical access controls; and
- Identify areas of potential weaknesses in controls.

Approach

Each of the following scope areas shown below describes a set of control objectives which should be met.

Physical access policies should provide for selective access to certain people at certain times and deny access to others. This also includes vulnerable and sensitive areas and the monitoring of staff and visitors.

The computer facilities and vault environment should be protected so that hazards, both man-made and natural would not affect their uninterrupted use. Environmental hazards relate to such areas as exposure to natural phenomena and the impact of nearby businesses.

In particular, there should be policies and procedures to protect against Fire and Flood damage (as the most common of the environmental hazards).

Overview

Physical Security is one of the most basic and commonly addressed form of data processing control. Sensitive areas include computer operations, general work areas and areas housing essential support systems such as air conditioning, telecommunications equipment, power control panels and tape or disk storage areas.

Good physical security planning includes consideration of threats to the computer site and vault and securities dealing areas from natural disasters, human error, accidents, vandalism and theft.

Physical security concerns itself with the prevention of unauthorised physical access to a site and the implementation of security devices and procedures to prevent disaster or damage to the computing environment or securities.

The two basic areas of potential vulnerability under the umbrella of physical security are:

- Physical access;
- Fire and flood protection.

Control of physical access provides the ability to grant selective access to certain people at certain times and deny access to others. The organisation should normally address the question of restricting access to the areas housing computer equipment and securities.

Controls for other vulnerable and sensitive areas such as telephone lines, power sources and air-conditioning should also be addressed. Personnel monitoring for both visitors and employees (including security and maintenance personnel) who may require access to restricted areas is another area that should be considered.

These controls can use a wide range of devices and techniques; the applicability would vary from site to site depending on the facility and the value of the data assets. Appropriate backup systems should be in place to recover from a power failure or a disaster disabling access controls.

The implementation of physical security measures often leads to the following general concerns:

- Contract security staff are inexperienced and may allow security standards to lapse;
- Administration of access lists does not take place regularly resulting in inappropriate access rights; and
- Periodic testing of the various alarm and detection equipment does not occur.

Our review of Physical Controls was of the security around the trading, safe custody area and software development environments and securities.

3.3.2 RECOMMENDATIONS

3.3.2.1 Physical Access Controls

The controls over physical access should be reviewed to ensure that only authorised individuals are allowed access to the installation under appropriate management review and supervision.

The review considered in particular :

- Sensitive and vulnerable areas should be identified and perimeter controls should be in place.
- Entry and exit point identification and control.
- Access Authorisation Procedures and Monitoring Devices. Access authorisation procedures should be used for all persons requiring access to sensitive areas such as employees, outsourcing agencies, security staff and visitors.

Following recommendations are made:

Vault Operations

3.3.2.1.1 Issue guidelines for key management in vaults and ensure they are followed.

Detailed procedures and guidelines to be followed by persons who hold the keys of the vaults are not explicitly set out.

Lack of clear procedures has led to non-standardised procedures being followed according to the perceptions of Manager Custody from time to time. This has led to person dependence. Under the circumstances, such a situation could result in disruption in operations due to non-availability of specific personnel.

Dual control should be introduced in vault operations wherever possible.

The "Guardwel" cabinet keys where the master keys of the bins are kept and locked in the evening should be locked by two different persons and at no point of time should both the keys be available with a single person.

The primary keys (both of first and second floor of Vikhroli) and the duplicate keys of the bins are kept in a "Guardwel" cabinet. Consideration should be given to storing the duplicate keys in a bank locker of a nearby branch.

Further, No.1 and No.2 keys of the "Guardwel" cabinets, where the duplicate keys of all the bins are kept should be with two different persons. (At present, both 1 & 2 keys are with Senior Manager - Custody, one set should be taken over by another person).

The same procedures should be implemented for Gulistan, Temporary Bins in Ground Floor of Vikhroli and the temporary bins of Mittal Court.

3.3.2.1.2 Strengthen security measures at Gulistan Vault.

The security level at the vault at Gulistan is low. Though no new pouches from last year have been added, we understand that the number of certificates in Gulistan is in the region of 50,00,000. We observed that there is no fire, smoke, heat detectors or alarms. Some times the certificates are kept in cabinets which are not fire proof. There exists a pit in the middle where water is collected during the monsoon and pumped out using a pumpset.

Flooding, during monsoon, in the event of the pumpset failing, is a distinct possibility.

If this Vault is to be continued, smoke, fire and heat detectors should be installed. The door separating the Vault area and the working area should be locked at night and the keys kept with security.

3.3.2.1.3 Strengthen Security measures in Vikhroli Vault area.

All the doors of the SHCIL offices are made of glass with no shutters. The vault room at Vikhroli has an electronic door, half of which is made of glass. Each vault has two entrances in Vikhroli site, one near the lift and the other general one. The vaults have been provided with an emergency exit also. In the Vault Room, there are no safe or steel doors to lock at night.

Since all the doors are made of glass, it gives a fair chance to break open into the vault room. The emergency door if not guarded and controlled, provide unauthorised entry point at night. Further, more than one entry point evokes concern.

It is suggested :

1. Strong doors with shutters need to be provided at all entry and exit points in all the floors which should be closed at night.

2. In first floor and second floor vault partition should be provided with strong room doors similar to that in banks which should be locked by two authorised responsible persons after the day's work is over.
3. The keys should be retained by the person locking the main strong room door. It should not be left in a desk drawer as is the present practice.
4. The duplicate keys of these strong room doors should be deposited in a locker in the nearest bank branch. Senior personnel (AVP or higher) could be authorised to operate the locker, in the event of an emergency.
5. Replace all glass doors in the Vault Area, with secure metal doors, and close second door near the lift on the first and second floors.

3.3.2.1.4 Strengthen security of the computer system controlling the vaults.

The racks in the vaults can be opened only by the custody personnel by means of a PC after identification through user-id and password. The person opening the rack can only close the rack after his job is over. The password and security of the system is important for safety of the securities. The security level appears weak and needs to be strengthened.

It is recommended :

1. The password file should not be available to all the users.
2. The name of the password file should not be easily discernible.
3. No user should have an access to C: and the system by default should display the application screens.
4. The password should never be kept in clear text. It should be encrypted.
5. The log of accesses generated by each PC should be reviewed by the Manager of Custody periodically and backed up every month for all the eight PCs.

3.3.2.1.5 Restrict access inside Vaults only to the custody personnel.

At the time of review, it was observed that many departments were using the bins inside the vault to keep their overnight securities. Keys of the Guardwel were given to them by the custody team.

Giving access to several individuals is a cause for concern.

The vaults should be locked at the end of each working day. Separate guardwell outside the vault housing temporary bins should be provided to users for overnight security keeping.

Other Operations

3.3.2.1.6 Avoid storage of securities in open racks or non-fire proof cabinets.

The Lodgment Team is located on the second floor and the temporary bins are located on the ground floor. It was observed that at the end of the day, the securities under processing were kept in the HRD room in racks or cupboards which are not fire proof.

Keeping the securities over night in racks or ordinary cabinets is risky.

The securities should be kept in a fire proof cabinets/vaults.

3.3.2.1.7 Formalise access authorisation procedures and restrict visitors from sensitive / vulnerable areas.

It was observed at Mittal court that the representatives of clients and brokers were issued passes enabling them to deliver securities and accept securities from SHCIL. The present practice does not include frequent verification with the original client / broker about the genuineness of their representatives. It was also observed that no formal practice existed for verifying the signatures of SHCIL personnel on the visitor's slip.

Loss or misuse of scrips by unauthorised person may result in pecuniary loss to SHCIL and jeopardise its reputation.

It is recommended that formal procedures be initiated for verification of authorisation letter from the original clients / brokers. Further, the security staff should be formally briefed to verify the signatures on the visitor's slip.

3.3.2.1.8 Pouch level audits should be conducted at more frequent intervals.

At the time of our review, it was understood that the pouch audits are performed throughout the year. However, management has not prescribed any time limit for completing the pouch level audit. Continuing with the present volume of business, it is predicted that the period between audit of a pouch may be as long as 15 months. The existing custody team, during their lean period of business, take up this pouch level audit. No defined period is maintained to start and finish the audit. Further, we were informed

that in many cases the loss of securities actually occurred during 1994 and were being reported as late as 1996.

Pouch level audit, if not done frequently may result in not locating, erroneous placement of scrips in wrong bins due to human errors or otherwise. Under the present practice, it may take a long time to detect such irregularities. At present, it may take an indefinite period to be sure of the loss prior to filing a Loss information Report/First Information Report. Further, the insurance claim may become invalid.

Pouch level audit should be done for all bins at more frequent intervals.

3.3.2.1.9 Formalise procedures to restrict access to the sensitive swipe card issuing machine kept in the control room.

At the time of our review, it was observed that swipe cards are issued to all employees to gain access to particular rooms. When an employee is recruited, a swipe card is issued by security based on letter from HRD. At present these card issuing machines are accessed by many individuals.

It is believed that such an easy access to the machine issuing swipe cards may result in an unauthorised employee gaining access to sensitive / vulnerable areas.

It is recommended that issue of swipe cards be centrally controlled by security staff only. Entry to sensitive areas like vaults should be restricted to employees with related responsibilities and random checks should be carried out. Further, it is recommended that the Kobra system which generates report of swipe cards that accessed the vaults in a particular day, be reviewed daily to determine if there were any violations or attempted violations and to take whatever follow up actions that are appropriate.

3.3.2.1.10 Central security room should be manned by security at all times.

At the time of our review, it was observed that the central security room is only manned during non working hours. The closed circuit TV is not being monitored during daytime.

Such lapses may result in security being compromised.

It is recommended that the central room be manned and all events monitored round the clock by security staff. The camera outputs should be viewed before destroying.

3.3.2.1.11 Strengthen control over physical movement of securities between locations

Movement of securities from Clearing House to Mittal Court, from Vikhroli to Mittal Court and between Mittal Court and Gulistan and the converse is done by armoured vehicles.

The movement of securities from Mittal Court to the premises of Outsourcing Agents is done using the vehicle of the agent. At this point of time, securities are still in street name and complete details are not available with SHCIL. In case of loss during this phase, building up the records for all the certificates, (though theoretically possible from Stock Exchanges records) is very difficult.

Also, the securities sent back from Outsourcing Agents to Vikhroli or Mittal Court after data entry and TD (Transfer deed) filling is over is done in the agent's vehicle.

Moving securities in ordinary vehicles maybe risky and leaves the organisation exposed to external threats.

It is recommended that movement of securities and TD's in and out of SHCIL premises should be done only by armoured vehicles.

It is also recommended that movement of blank TD's be avoided and relevant particulars of the Transferor and Transferee be endorsed.

SHCIL should endeavor to have the outsourcing agents perform their job within their own premises which would reduce unnecessary movement of securities and its risks there of.

3.3.2.1.12 Duplicate keys of bins of Gulistan Vault should be kept in safe custody.

The duplicate keys of the vaults and bins and the Guardwel cabinets are not kept properly. The keys were found in a cupboard which was not locked.

Should the duplicate keys fall into wrong hands it could compromise security. Loss of scrips may also go unnoticed.

It is recommended that all the duplicate keys should be accounted for and kept in a safe location. The missing keys, if any, should be identified and the locks to the bins that correlate to the missing keys, should be changed.

3.3.2.1.13 Safe keeping of objections securities should be strengthened.

The certificates which are returned with some objections are processed in Mittal Court and kept in the Gulistan Vault during nights. These securities are kept in Guardwel fire proof cabinets. The keys are maintained by Objections department only and not handled by custody team. During a recent internal audit more than 100 pouches were found to be missing.

The number of missing pouches is high considering the volume of objections to the actual custody volume. If this problem is not solved and analyzed, this may lead to client dissatisfaction.

The security for the objection securities should be strengthened and the periodical stock verification should be done by the objections department for such securities.

3.3.2.2 Fire/Flood Controls

Fire and flood, along with the resultant damage caused by fire extinguishing procedures (such as smoke and water damage) are two of the most common causes of damage to data processing equipment and records.

Following recommendations are made:

3.3.2.2.1 Install Fire/Smoke/Heat detectors at Gulistan and Mittal Court.

At the time of our review, it was observed that there was no smoke detectors, heat detectors and fire alarms installed at Gulistan and Mittal Court.

Lack of heat/smoke detectors, fire alarms may result in loss of data, securities and business.

It is recommended that smoke and heat detectors be installed in every room with the facility of a central panel monitoring system. Adequate audio and visual alarm informing the site of fire should be provided in the fire panel monitoring system.

3.3.2.2.2 Review and test adequacy of fire extinguishers.

At the time of our review, fire extinguishers were not regularly checked to see if these were out of date, empty or all in place.

In the event of a fire, SHCIL may have fire extinguishers that do not work. Such a situation could, in addition to causing financial loss, lead to loss of life.

It is recommended that steps be taken to ensure that the fire extinguishers be regularly reviewed for adequacy and appropriateness and tested from time to time.

3.3.2.2.3 Practice fire drills at all locations.

At the time of our review, no fire drills were practiced by SHCIL personnel.

In the event of a fire, SHCIL personnel may not be in a position to cope with the situation. This could in addition to causing financial loss, lead to loss of life.

It is recommended that fire drill procedures be laid down. Also, documented records of regular, ongoing testing and maintenance of equipment and testing of evacuation procedures should be maintained.

3.3.2.2.4 Train staff members in usage of fire extinguishers at all locations.

Whenever a fire or natural calamity strikes, it may not be prudent to depend on security personnel only. We understand that the SHCIL staff are not conversant with the use of fire extinguishers. Regular fire drill practice will build confidence to use the fire extinguishers and would serve its intended purpose when fire breaks.

Without training the fire extinguishers may not serve its purpose because the affected person are ignorant of its use. This may lead to loss of human life too.

First the security personnel should be trained in using the fire extinguishers and thereafter each member of the staff should be trained to use the fire extinguishers.

3.3.2.2.5 Initiate steps to eliminate break of an electrical fire at Vikhroli.

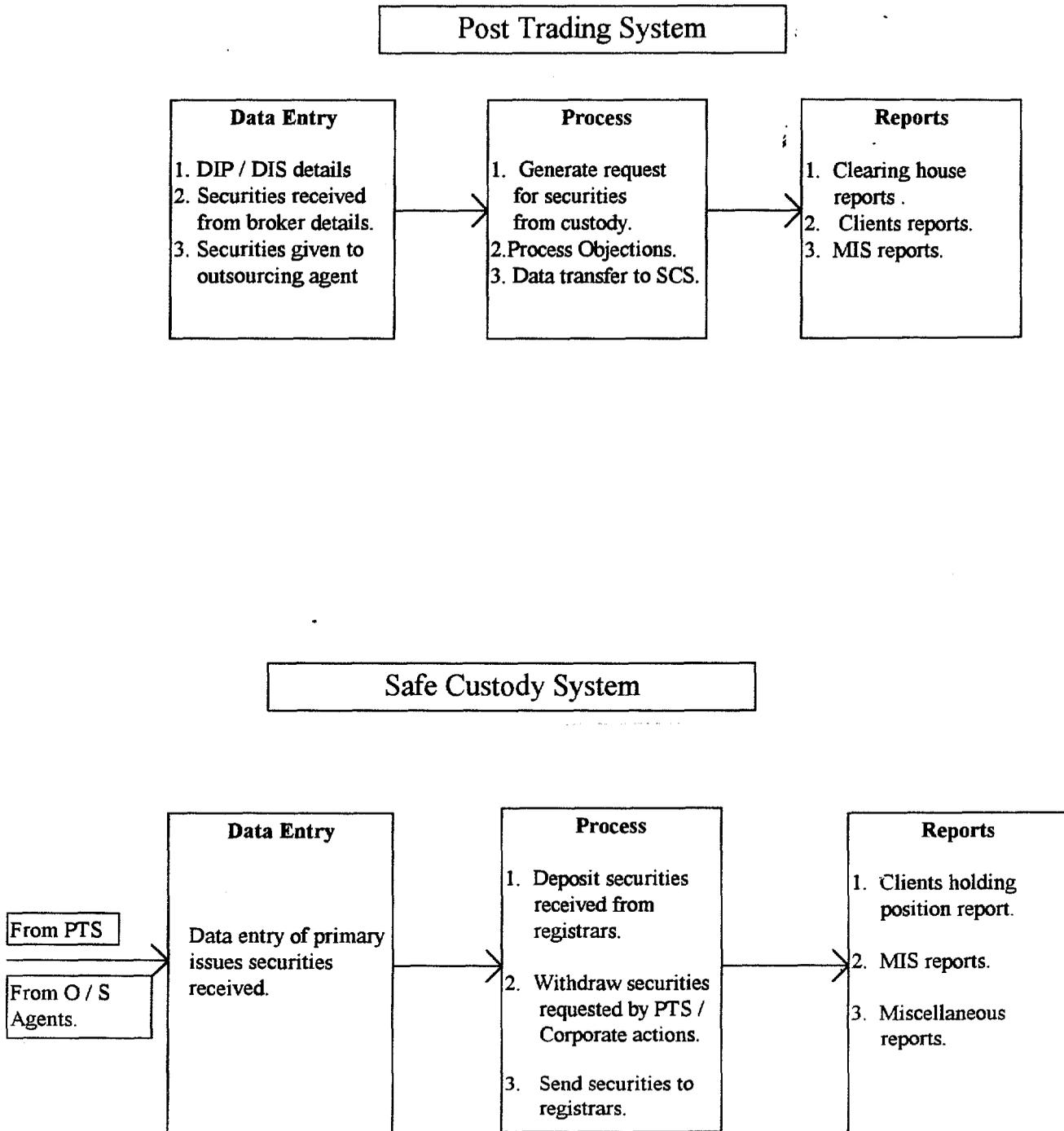
At the time of our review, it was observed that there existed no procedure at Vikhroli, at the end of each working day, to cut off electric supplies to those rooms where no work is in progress.

Accidental short circuits may occur when lights, fans, air conditioners etc. are running unattended in those rooms where no work is going on. In case of fire, wooden cabinets would act as catalysts to the spread of fire.

It is recommended that a central circuit breaker panel be installed which can be de-energised after each working day to switch off incoming supplies to all rooms where no work is in progress. A person should be made responsible for switching off breakers.

4. SAFE CUSTODY SYSTEM (SCS) & POST TRADING SYSTEM(PTS)

4.1 Process Cycle for PTS and SCS



4.2 Recommendations

4.2.1 Strengthen controls over access to the application system by users.

The access to the application is controlled through various tables. However, we found that these tables are not updated on a timely basis. For example, on a selected day, there were 8 authorised users listed on one table, and 17 authorised users listed on a second table, but there were only 7 users in the department. One authorised user who was a Manager, had resigned approximately 6 months previously.

Giving access in excess of a user's needs could be risky.

It is recommended that unauthorised users found in these tables should be made inactive or deleted. Other user access profiles should also be reviewed, to ensure that the privileges granted are commensurate with their job responsibilities.

4.2.2 Provide user access to the PTS application only on "need to know, need to do" basis.

In PTS, various users from corporate actions, B Group purchases, sales, NSE purchases and sales access various screens depending on their needs. However, all these users are given access and are able to update all the screens.

Such free access could compromise the integrity of the standing data.

It is recommended that the users should be given access permissions according to need to know basis only.

4.2.3 Differentiate maker and authoriser of a transaction; preferably authoriser should be one level higher.

The DIP (Delivery Instructions for Purchase) and DIS (Delivery Instruction for Sale) details are the primary entries which initiates the chain of actions in SHCIL. The data entry made by one individual can be authorised by the same person. This defeats the very purpose of introducing one more level of authorisation. The data received on a floppy from clients is not verified or authorised by this department.

The system should not allow the maker to authorise his own transactions. It is preferable for an individual one level above to authorise the same. Likewise, data received on floppy should be authorised.

4.2.4 Enforce accountability amongst various "DIP" users.

There are seven to eight persons in DIP/DIS department. All of them use the "DIP" user-id and password.

If it is not possible to determine who has entered a record at a later stage, the very purpose of capturing the user-id of the user entering the transaction is defeated.

It is recommended that the user-id of the individual entering the transaction should be captured in the user-id column only and not in the last updated user-id column.

The usage of a generic user-id like "DIP" should be stopped.

4.2.5 Obtain daily report of cheques received and held by the collection agent.

The corporate actions department in Mittal court is responsible for the collection of monies on behalf of its clients. SHCIL utilises the services of the Skypack Financial Services to collect the cheques. No monitoring mechanism exists to ensure that the agent deposits the cheques collected on due dates.

If the cheque is collected but not credited to the client account on due date, it would lead to client dissatisfaction and embarrassment to SHCIL.

The department should ask the collection agent to provide a list of cheques collected by the company daily in a report with due date for lodging in the Bank.

This should be used as a control report to ensure that the cheque received is deposited on the due date and it is not missed due to some clerical error at the agent's office.

4.2.6 Develop and maintain adequate systems and operations documentation.

Operations and systems documentation are not adequate.

The absence of adequate documentation leads to over-dependence on key individual. This may even result in the risk of not being able to operate the system in the absence of such individuals. Furthermore, the learning curve for new staff is considerably longer in the absence of adequate documentation.

It is recommended that high priority be accorded to the preparation of adequate documentation.

5. BUSINESS CONTINUITY PLANNING

Business Continuity Planning may be defined as the identification and protection of critical business processes and resources required to maintain an acceptable level of business, protecting those resources and developing procedures to ensure the survival of the organisation in times of business disruption.

5.1 PURPOSE, OBJECTIVES, APPROACH AND OVERVIEW

Purpose

To evaluate the organisation's ability to continue in operation under adequate security protection in the event of an extended disruption.

Objectives

- Confirm that the provisions, procedures and staffing have been established to support recovery from an extended disruption;
- Conclude as to the adequacy of the business continuity plan; and
- Identify areas of potential weakness or omissions in the business continuity plan

Approach

Each of the following scope areas shown below describes a set of control objectives which should be met.

- The plan should provide for recovery from different levels of business disruption, should describe how to use and activate the plan and should provide for testing and maintenance of the business continuity plan.
- Recovery should be adequately addressed through the Business Continuity Team Composition and Functions. Team members should include representatives from all relevant areas of the organisation and team functions must be well-defined.
- Application Software and Data File Priorities and minimum recovery time frames should be established on the basis of financial and operational impacts of computer processing interruption.
- The Equipment Inventory and Critical Configuration information needed to rebuild the data center and run the application systems should be identified.

- The Communications Requirements in terms of equipment and software needed to rebuild the data center and the communications components required to support processing of critical application systems should be identified.
- The Systems Software Inventory and Critical Configuration required to support critical hardware and communications configurations should be identified.
- Critical Forms and Supplies needed to process critical applications and supplies needed for computer operations should be identified. Vendor contacts and lead times should be documented.
- Backup Provisions for Software, Data Files and Supplies as well as off-site rotation procedures should be adequately planned and executed to facilitate recovery of critical applications in the event of an extended disruption.
- Alternative Processing Facilities which provide for restoration of critical application system processing within minimum recovery time frames and availability of suitable equipment, communications and systems software configurations should be identified.
- Transportation, Inventory and Logistics regarding vehicles and alternative sources of obtaining those vehicles should be documented. Logistical tasks of relocating data processing operations should be defined.
- Security Provisions should be made to ensure continued security protection of data access paths during operation of alternative facilities.
- The scope of Business Continuity Plan Testing plans should be adequate to ensure restoration of data processing operations within minimum recovery time frames and completion of trial executions of the plan on a regular and frequent basis.
- Business interruption insurance and alternative facilities and all possible data processing risks should be identified and evaluated and insurance should be adequate to cover the loss resulting from suspension / delay of operations.

The BCP is analysed in terms of gaps where the state of readiness of the BCP is insufficient to facilitate recovery of data processing operation under adequate security protection in the event of an extended disruption.

Overview

A business continuity plan is a business management plan rather than a technical plan. Hence, continuity planning is based on the understanding of the organisation, identifying the tools that support the operations of the business, evaluating the loss of such tools, knowing who would handle a crisis situation and how would they do that.

It is essential in today's business environment for an organisation to consider what should be done if a disaster were to have an impact upon the organisation's normal business environment, since a minor, major or catastrophic disaster could bring substantial losses to any business.

The ongoing business is based on the assumption that the improved services, productivity and opportunities for growth provided by the current technology implemented within the organisation would not decline. It is therefore important that the dependency of the organisation on technology be considered by the organisation in identifying the critical portions of the business.

Managers of the business are custodians of the business interests and responsibilities. They must practice good stewardship, which includes operating in a way that preserves profitability, stability and quality and advances the interests of customers, employees and investors. Management cannot be said to be fulfilling this duty if an unplanned event can jeopardize the survival of the organisation.

The following risks and issues are raised in the absence of effective BCP:

- Business interruption resulting in inability to serve the current customer base, erosion of customer base, lost opportunities, loss of goodwill, and inability to compete;
- Financial loss due to inability to process transactions;
- Legal liability resulting from failure to satisfy contractual obligations; or
- Going out of business.

Just having addressed the issue of business continuity planning is not enough. A business continuity planning project must involve the entire organisation. Time and resources must be provided by management for the development, initial and ongoing testing and ongoing maintenance of the plan. Unless management commitment is displayed, the whole organisation is involved and the plan development project is given a high priority, the project is likely to fail.

Plans in the past have generally addressed only computer-related disasters. However, this is too narrow a focus and all of the related business activities should be addressed to ensure business continuity, including manual records and information.

The scope of the business recovery plan within the organisation must also be determined. This would depend on the structure of the organisation, such as a multiple or a single facility. The most important aspects of a successful approach to business continuity planning are paying attention to detail and addressing small sections at a time.

A pragmatic or common sense approach to protection should be used in the BCP, through addressing the critical processes of a business. Total security or protection over every facet of the business is either unattainable or prohibitively expensive.

Given the above, and in view of the high dependence on technology driven Information Systems for business operations, SHCIL recognizes the need for a Business Continuity Plan. At the time of our review there was no plan in place. At Mittal Court the Security Department has prepared an approach paper for action in case of Fire and bomb threat. But it can only be a starting paper for the final plan. The system department also has some ideas/ points written about BCP. It is understood that a coordinator is to be appointed and representatives nominated from each department to assist the coordinator on aspects concerning their respective departments.

The coordinator would be required to be assigned full-time to the plan preparation process.

The basic approach to be adopted by the recovery team could be summarized as :

- identify business recovery requirements;
- understand the limitations of the main production environment (PYRAMID NILE) and other key technology components; and
- arrive at the minimum and maximum recovery time, given the limitations of the technology components.

The scope of our exercise was to review the arrangements and make recommendations in the broader context of business continuity planning as opposed to computer disaster recovery or disaster contingency planning.

Business continuity planning involves taking a business process view. Detailed aspects include :

- understanding the business processes and their criticality in the short run (including impact on business if the process is not available for specified time periods) and maximum acceptable recovery timescale;
- identifying resources (computer based and non-computer based) used by each business process;
- evaluating threats faced by each resource (including probability of occurrence and its likely impact); some ground work has been done by the Security department.
- designing countermeasures against the threats;

- classifying potential disasters;
- developing emergency procedures;
- selecting teams and defining responsibilities;
- developing detailed procedures for movement to and recovery at alternate site, damage assessment and shift back to home site;
- maintaining contact lists (staff, vendors, service providers, customers etc.) and backup resources;
- testing and on-going maintenance of plan;
- circulating the plan among appropriate people;
- keeping a copy of the plan off-site.

Our recommendations have been arrived at considering the need for achieving full recovery of critical business processes within acceptable time frames; and have been classified under two sections - approach and critical exposures.

5.2 RECOMMENDATIONS

5.2.1 APPROACH TO BUSINESS CONTINUITY

5.2.1.1 Address both computer disaster contingency, manual records and information to ensure business continuity.

The planning process should consider the business process requirements for operating out of the stand-by location (i.e. trained people, computer and non-computer based resources etc). A business impact analysis should be the first step in the planning process. This should result in the definition of acceptable recovery time scales for each critical business process. To achieve these timescales, resource requirements should be identified and different options developed. Appropriate resource options should be selected based on the cost of each option compared with the business requirement. The process should consider disaster avoidance measures, apart from recovery steps. Recovery steps should also be planned for operational disruptions (e.g., telephone lines downtime, absence of key personnel), which do not require a shift of location. Based on the selected resource options, teams should be selected, responsibilities defined and detailed procedures documented and databases prepared. Training, plan testing and maintenance should also be considered in the planning process.

5.2.1.2 Clarify project sponsorship and ownership and define project management organisation structure and procedures.

For developing a focused, comprehensive and effective business continuity plan within an acceptable time frame, high commitment and active participation is required from senior management. Several key decisions need to be taken on recovery priorities, acceptable recovery time-frames and consequently the extent of redundancy to build in. Typically, significant costs are involved, particularly because a stand-by "hot-site" would mean duplicating major resources. It therefore follows that the "project sponsor" needs to be the Managing Director.

To prepare an effective business continuity plan, managers of critical business processes need to invest time on the project, as they are best equipped to define their minimum resource requirements and recovery timescales. In the event of a shift to the stand-by location, it is the business process managers who would be directly affected. In view of this, a cross-functional steering committee comprising functional heads is considered to be the best method for ensuring proper project commitment, focus and management. The steering committee should be the "owners" of the business continuity planning project.

It is therefore recommended that project sponsorship and ownership be formalized and a high-level steering committee be set up to provide oversight to the project.

5.2.1.3 Follow a detailed methodology for business continuity planning.

Business continuity planning is a complex, multifaceted process that requires the support of the entire organisation.

- **BUSINESS IMPACT ANALYSIS**

Identifies business processes and activities, decides on criticality of business processes (based on quantitative as well as subjective methods), arrives at recovery priorities and target recovery time scales, identifies resources (computer based and non-computer based) used by each business process and the minimum resources required for business continuity, analyses threats to resources, the current risk reduction measures for the threats and recommends further counter-measures.

- **STRATEGY SELECTION**

Develops different strategy options for meeting business continuity requirements identified in earlier stage. These strategy options are in terms of backup or alternate resources (stand-by site, computers, telecommunications etc.) and the costs of each option. The decisions required are based on the degree of preparation, which is in turn

5.2.1.2 Clarify project sponsorship and ownership and define project management organisation structure and procedures.

For developing a focused, comprehensive and effective business continuity plan within an acceptable time frame, high commitment and active participation is required from senior management. Several key decisions need to be taken on recovery priorities, acceptable recovery time-frames and consequently the extent of redundancy to build in. Typically, significant costs are involved, particularly because a stand-by "hot-site" would mean duplicating major resources. It therefore follows that the "project sponsor" needs to be the Managing Director.

To prepare an effective business continuity plan, managers of critical business processes need to invest time on the project, as they are best equipped to define their minimum resource requirements and recovery timescales. In the event of a shift to the stand-by location, it is the business process managers who would be directly affected. In view of this, a cross-functional steering committee comprising functional heads is considered to be the best method for ensuring proper project commitment, focus and management. The steering committee should be the "owners" of the business continuity planning project.

It is therefore recommended that project sponsorship and ownership be formalized and a high-level steering committee be set up to provide oversight to the project.

5.2.1.3 Follow a detailed methodology for business continuity planning.

Business continuity planning is a complex, multifaceted process that requires the support of the entire organisation.

- **BUSINESS IMPACT ANALYSIS**

Identifies business processes and activities, decides on criticality of business processes (based on quantitative as well as subjective methods), arrives at recovery priorities and target recovery time scales, identifies resources (computer based and non-computer based) used by each business process and the minimum resources required for business continuity, analyses threats to resources, the current risk reduction measures for the threats and recommends further counter-measures.

- **STRATEGY SELECTION**

Develops different strategy options for meeting business continuity requirements identified in earlier stage. These strategy options are in terms of backup or alternate resources (stand-by site, computers, telecommunications etc.) and the costs of each option. The decisions required are based on the degree of preparation, which is in turn relate to the target recovery timescales.

• **PLAN PREPARATION**

Defines key personnel and responsibilities, details procedures for disaster declaration, emergencies and recovery, develops database of personnel, resources, vendors, service providers etc. Training is also provided to all personnel.

• **PLAN TESTING AND REVISION**

An on-going process of testing one or more components of the plan in different degrees of simulation and revision of the plan in view of test results.

To carry out tests effectively the following steps should be adhered to:

- Develop test plan
- Perform test
- Document test results
- Evaluate test results and consider revision where necessary

• **PLAN MAINTENANCE**

Maintenance of any plan should include adequate update procedures to reflect any changes to the organisation or to the technology components. Specifically, there should be mechanisms to report and incorporate key personnel changes and system changes.

• **PRIORITY LEVELS TO ASSIGN**

As every business process is not critical in the event of a disaster - levels of priority may be established on the basis of financial and operational impacts. Consideration should be given to at least the following:

CRITICAL AREAS	VITAL CRITERIA FOR RECOVERY
Application Software and Data files	Time taken to recover
Equipment and Configuration	Vendor plan for expediting
Communications	Vendor plan for expediting
Systems Software and Configuration	Vendor plan for expediting
Critical Forms and Supplies	Vendor plan & lead time for expediting
Backup Provision for Software, Data & Supplies	Off-site maintenance procedures
Alternative Processing Facilities	Manual, Cold or Hot Site or Reciprocal arrangements
Transportation and Logistics	Procedures for input collection and output distribution
Security Provisions	Access control procedures at alternative facilities.
Test Plan	Staff familiarity with assigned responsibilities
Insurance Coverage	Adequate to cover business interruption and alternative facilities.

In an established methodology, each of these stages are expanded into several detailed activities, steps and guidance checklists.

In the absence of a detailed methodology, it is difficult to ensure an exhaustive and practical plan.

It is therefore recommended that a methodology be acquired for business continuity planning.

5.2.1.4 Acquire software tools for business continuity planning.

Several software tools which support business continuity planning are available. The functionality provided by these tools includes assistance in carrying out a business impact analysis using quantitative techniques, repository for detailed plan procedures, databases for storing details of personnel, equipment, vendors etc.

The main advantage of using a software tool is that plan maintenance is greatly facilitated. Generally, the tool keeps track of dependencies, hence if a resource undergoes change, the software tool updates the changes in all relevant parts of the plan. These software tools also provide rapid information retrieval facilities.

It is recommended that a software tool be acquired to facilitate business continuity planning.

5.2.2 CRITICAL EXPOSURES

5.2.2.1 Action contingency plans for equipment.

The main service provider, Siemens Equipment has no contingency plan for SHCIL, should there be a disaster. The other service provider, Microland, has no contingency plan either.

Without a contingency plan from the service provider, SHCIL may not be able to process the necessary data.

It is recommended that the contingency plans for equipment be actioned.

5.2.2.2 Document telecom network.

There is no documentation for the telecom network or procedures for its recovery.

In the case of a disaster, considerable time would be lost in trying to determine the configuration. This could lead to an inordinate delay in the recovery of operations.

It is recommended that the telecom network be documented and regularly updated and recovery procedures be initiated and documented.

5.2.2.3 Backup critical paper-based records.

There are no backups of critical "paper-based" records and documents.

In the event of a disaster affecting the home site, business processes would find it difficult to function without certain documents. Loss of such documents may even lead to financial losses.

Consideration should be given to preparing photocopy or micro-film or digitized backups of all critical paper-based records. These backups should be stored off-site in fire proof cabinets.

Binwise pouch list, clientwise and scripwise, should be taken every month and kept as a backup. If the system is not available for an extended period, the list can be used to retrieve pouches from the bins.

5.2.2.4 Setup communications with emergency services.

SHCIL does not have any direct communication setup with the police department services or a hospital.

In the absence of such a provision, delay would be caused to take remedial measures, in an emergency.

Given the nature of the business and the criticality of SHCIL to its clients, a hot-line and/or direct alarm connection could increase the speed of response in case of an emergency such as a fire or terrorist attack. It is therefore recommended that some form of direct communication be setup with the emergency services.