Sample Information Systems Audit and Forensic Audit Report

The Institute of Chartered Accountants of India
(Set up by an Act of Parliament)
New Delhi

Sample Information Systems Audit & Forensic Audit Report

The Institute of Chartered Accountants of India
(*Set up by an Act of Parliament*)
New Delhi

Edition : September, 2016

Committee/Department : Committee on Information Technology

Email : cit@icai.in

Website : www.icai.org/http://cit.icai.org

Price : ₹ 100/-

ISBN :

Published by : The Publication Department on behalf of Committee on Information Technology,
The Institute of Chartered Accountants of India,
Post Box No. 7100, Indraprastha Marg,
New Delhi-110 002.

Printed by : Sahitya Bhawan Publications, Hospital Road,
Agra 282 003.

September/2016/1000 Copies

Foreword

Information Technology plays a vital role in supporting the activities of any organisation. The growth and change that has come about as a result of developments in the technology have important implications. These technological changes have put more focus on the role performed by the Chartered Accountants, especially in the fields of Information Systems Audit and Forensic Accounting.

Recent financial and cyber frauds have emphasised the urgent need for a transparent and clean system. The vital problem encountered by some of the Chartered Accountants is the lack of practical exposure in the area of Information Technology. They are faced with various issues while implementing the acquired knowledge with the actual working environment like how IS Audits & Forensic Audits are conducted, how the report is to be prepared, how the evidences gathered are to be dealt with in the reports.

Identifying "Information Systems Audit" and "Forensic Accounting & Fraud Detection" is one of the niche area, the Committee on Information Technology is conducting a Post Qualification Course on "Information System Audits" and a Certificate Course on "Forensic Accounting and Fraud Detection". The course aims to develop such skills that are required to uncover corporate / business frauds, measure resultant damage, provide litigation support outside counsel by applying accounting, auditing principles for the detection of frauds.

This publication on "Sample IS Audit & Forensic Audit Report" will enable Chartered Accountants both in practice and in industry serve as Information System and Forensic Auditors, in preparation of IS Audit and Forensic Audit report.

I appreciate the efforts put in by CA. Atul Kumar Gupta, Chairman, CA. Manu Agrawal, Vice-Chairman and other members of Committee on Information Technology for bringing out this publication as guide for IS Audit and Forensic Reports.

I am sure that it will be a useful learning material.

Best wishes,

CA M. Devaraja Reddy
President, ICAI

Preface

Information Technology has now emerged as the Business Driver of choice by Enterprises and Government Departments to better manage their operations and offer value added services to their client/ citizens. While the increasing deployment of IT has given immense benefits to enterprise and government departments, there have been increasing concerns on the efficiency and effectiveness of the massive investments made in IT, apart from the safety and security of Information Systems themselves and the data Integrity.

The Post Qualification on Information Systems Audit aims to equip members with unique body of knowledge and skill sets so that they become Information Systems Auditors who are technologically adept and are able to utilise and leverage technology to become more effective in their work and learn new ways that will add value to clients, customers and employers.

Forensic Accounting has come into limelight due to rapid increase in financial frauds and white-collar crimes. The integration of Accounting and investigative skills creates the speciality known Forensic Accounting. Forensic Accounting uses accounting, auditing and investigating skills to conduct investigations, and thefts and frauds cases. The job of Forensic accountants is to catch the perpetrators of the financial theft and frauds including tracing money laundering, identifying theft activities as well as tax evasions.

The Certificate Course on Forensic accounting and Fraud Detection is a blend of theoretical and practical training and is intended to equip the participants with concepts in Forensic accounting which aims at sensitizing Fraud Investigators, Auditors, security Professionals, and IT executives about the risks and mitigation strategies for an effective business environment. It provides an incisive analysis of how fraud occurs within an organisation and the latest techniques of finding it.

It gives us immense pleasure to bring this publication on “Sample IS Audit and Forensic Audit Report” for the members active in the Information Systems Audit and Forensic Audit field(s). This learning guide is prepared to assist the professionals to prepare IS AuditsReports and Forensic Audit Reports. It is brought out to enhance the learning experience and to synchronise the theoretical knowledge with the practical aspects. It will thus provide increased understanding as to how to prepare the reports while conducting Information Systems and Forensic Audits. It provides a well-knitted overview of the format of IS audit report and Forensic reports.

We would like to express our gratitude to CA M. Devaraja Reddy, President ICAI and CA Nilesh S. Vikamsey, Vice President ICAI for their continuous support and encouragement to the initiatives of the Committee. We must also thank my colleagues from the Council at the Committee on Information Technology for providing their invaluable guidance as also their invaluable dedication and support to various initiatives of the Committee.

We would also like to extend our sincere thanks and appreciation to Mr. S. P. Shah Singh, Mr. Vinay Saini, CA Sanjay Gupta, CA Naresh Gandhi and CA Ashish Makhija who contributed their expert knowledge for this publication brought out by the Committee on Information Technology. We really appreciate their sincere efforts and dedication towards the work of the Committee.

We wish to express our thanks to Committee Secretariat in giving Final shape to the publication.

CA Atul Kumar Gupta
Chairman
IT Committee

CA Manu Agrawal
Vice-Chairman
IT Committee

Index

IS Audit Report for ICAI

XXXXX LIMITED

Review of Information Systems
General and Application Controls

Draft Report
December 31, 9999
(FOR DISCUSSION PURPOSES ONLY)

Sample Information Systems Audit & Forensic Audit Report

XXXXX Limited

Information System Audit Report (For Discussion Purpose Only)

Review of System Management (Including General IT controls)

Table of Contents

A. Objective and Scope

Networks may have vulnerabilities that expose them to possible exploit or attack. These vulnerabilities -- both known and previously unknown -- often exist in the most unlikely of places, such as the firewalls, intrusion protection systems and other perimeter defenses ostensibly protecting the network. Just one vulnerability in a single product potentially exposes every other device and application on the network. Even if one of these systems is vulnerable, the integrity, confidentiality and availability of all information resources can suffer.

The objective of audit is to

- Identify the weaknesses in various device configurations that may put confidentiality, integrity and availability of data at risk and
- Provide high level recommendations to address these weaknesses.

B. Approach

The review is based on

- Hard and soft copies of network diagrams / configurations of various network devices provided to us
- Walkthrough of the configuration of firewall
- Walkthrough of the configurations of various servers
- Interviews of some administrators etc.
- but without
- Vulnerability scan., an automated technique that identifies weaknesses in the devices on network that are open to known vulnerabilities
- Penetration testing, a method for evaluating the security of a computer system or network by simulating an attack. The process involves an active analysis of the system for any potential vulnerabilities that may result from poor or improper system configuration, known and/or unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures. This analysis is carried out from the position of a potential attacker, and can involve active exploitation of security vulnerabilities. Any security issues that are found are presented to the system owner together with an assessment of their impact and often with a proposal for mitigation or a technical solution. The intent of a penetration test is to determine feasibility of

an attack, the amount of business impact of a successful exploit, if discovered

C. Introduction

XXXXX Limited has a large IT setup to provide IT related services to the company. It has in-house IT maintenance but FMS is outsourced to HP. There are more than 50 window based and 4 Unix servers in the data centre. ABC software is used to support finance function. Out of four Unix machines two are running HP-Unix and two are on AIX. These servers run own developed applications. Enterprise storage size is more than 30 TB. XXXXX Limited is using Multiple WAN links provided by Reliance, TATA etc. A mix of Nortel and Cisco network devices are used at XXXXX Limited.

D. Executive Summary

Our audit of the IT security controls of XXXXX Limited determined that:

- XXXXX Limited has established a security management program.
- XXXXX Limited has implemented controls to prevent unauthorized physical access to its facilities, as well as logical controls to protect sensitive information. However, we noted several opportunities for improvement related to XXXXX Limited's access controls:
  - Standardized access request forms are not utilized for managing information systems access;
  - There is no formal process for auditing logical and physical access privileges; and
  - There are no formal procedures for reviewing system logs.
- XXXXX Limited has implemented an incident response and network security program. However, we noted several areas of concern related to XXXXX Limited's network security controls:
  - A formal incident response procedure has not been established;
  - A firewall configuration standard has not been developed;
  - An outbound web proxy has not been implemented;
  - Controls are not in place to prevent unauthorized devices from connecting to the network and control the use of removable media;

  - Significant improvements are needed to the vulnerability management program;
  - A methodology is not in place to ensure that unsupported or out-of-date software is not utilized; and
  - Several vulnerabilities with known exploits were identified as a result of our independent vulnerability scans.
- XXXXX Limited has implemented a configuration management process to control changes made to its IT systems. However, there is no routine auditing of XXXXX Limited's server and workstation configuration.
- XXXXX Limited has documented contingency procedures that detail the recovery of servers in the event that normal service is disrupted. However, the contingency plan for workstations may not be feasible since it relies on a 3rd party without a service contract.

E: Observations and Impact – 1.0 NETWORK ARCHITECTURE / DIAGRAM

Sr. No	**Observation & Impact**	**Recommendation**	**Auditee Response & Implementation Timeline**
1.1	**Inappropriate Network diagrams** **Background:** Network diagram is depiction of a system in terms of individual points (which may represent a location, resource, status or task) and the links between them used to pass goods, services, data or other communications. It helps model the relationships of the links and the timing and direction of the flows between them. Proper documentation is very	Diagram should conform to standard conventions. They should be updated as and when changes occur to network.	

	important to an IT organization. Without it, there's no good way to transfer knowledge quickly when it's really needed and network diagram is one such document. **Observation:** a) Network diagrams do not follow diagramming conventions. It is not using the conventional device icons to represent devices like routers, L-3 switches etc.. b) The network diagrams do not present the exact network picture as it currently exists. Some devices that are not in use e.g. 'Domino SPIL' are still shown in the diagram. **Impact:** *Understanding the diagram may be difficult that may render maintenance difficult resulting in delays to fix problems. The availability of the network, therefore, may be at risk.*		

E: Observations and Impact – 2.0 SERVERS

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
2.1	**Vulnerable services not stopped** **Background:** a) Windows services	Identified vulnerable services should be reviewed for their usage and if not	

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
	represent a large percentage of the overall attack surface in Windows. Windows Service Hardening restricts critical Windows services from doing abnormal activities in the file system, registry, network, or other resources that could be used to allow malware to install it or attack other computers. Windows Service Hardening provides an additional layer of protection for services based on the security principle of defense-in-depth. Best practices recommend that unless required these services should be disabled / stopped because they may be exploited. **Observation:** a) Vulnerable/redundant services viz print spooler which loads files to memory for later printing, remote registry which enables remote users to modify registry settings, wireless configurations which provides automatic configuration for wireless adapters and telephony which provides Telephony API (TAPI) support for programs that control telephony devices),	required they should be stopped.	

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
	DHCP client which manages network configuration by registering and updating IP addresses and DNS names are running on servers listed below. • XXXXXX-DC01 - (Domain Controller) • XXXXXX-DC02 - (Additional Domain Controller) • XXXXXXCTX01 - (Citrix Meta Frame) • XXXXXXCTX02 - (Citrix Meta Frame) • ASER! - (Extranet Application Server) • EXTDB1 - (NB Database) • EDB2 - (NB Database) • FACTORY1 - (File Server) • XXXXXXAVDC - (Anti Virus) • XXXXXXISA - (ISA) • XXXXXXMAIL - (Exchange Server) **Impact:** *Some services may be exploited to yield confidential information while other may allow changes in configuration of the system that may put availability of the system at risk.*		

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
2.1	**Background:** b) Servers /network devices support a large number of network services. Some of these services can be restricted or disabled, improving security.. Good security practice for devices is to support only traffic and protocols the network needs. The information obtained using the identified vulnerable services isn't usually tremendously sensitive but it can sometimes be useful to an attacker who can use this information for launching denial of service attack **Observation:** b) Following vulnerable services are running on the servers listed below **Echo** – used for checking whether the device is working or not, **Discard** – a service that typically sets up a listening socket and will ignore all the data which it receives and is unused these days, **Chargen** – character generator service, **Finger** - provides information about a user on a system.	Identified vulnerable services should be reviewed for their usage and if not required they should be stopped.	

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
	The service provides user information, which may be extremely valuable for hacking. • MARC - (SPD Application) • IMAN - (RND Application) • BKPSERVER - (LEGATO Application) • SR1_DR - (Fail Over SR1) • SR2_DR - (Fail Over SR2) • SR3_DR - (Fail Over SR3) • SR4_DR - (ERP DB Fail Over) • CL01 - (Finance Payroll Application) • CL02 - (Production & Sales Support Application) • CL03 - (Material Spare Part Application) • SR1 - (Database server Finance system) • SR2 - (Database server Production & Sales Support) • SR3 - (Database server Material & Spares) • CL01_DR - (Fail Over CL01)		

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
	• CL02_DR - (Fail Over CL02) • CL03_DR - (Fail Over CL03) • CL04_DR - (ERP Application Fail Over) • QA02 - (ERP QA DB) **Impact:** *The information obtained using these services may sometime be used by attacker to launch denial of service attack that may render network service offered by the device unavailable to genuine user.*		
2.2	**Inappropriate screen saver settings** **Background:** Password protected screen saver automatically locks the screen after a defined period of inactivity on the machine. **Observation:** Screen saver is not enabled on servers listed below. XXXXXXCTX02 - (Citrix Meta Frame) ASER! - (Extranet Application Server) FACTORY1 - (File Server) **Impact:** *Servers remain open to unauthorized access when*	Screen server should be enabled.	

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
	unattended. The confidentiality of the data in these servers may be at risk.		
2.3	**Too permissive sharing on shared folders** **Background:** Sharing on folders on hard disk allows other people on the network to read and/or write files to the folder. It can be specified who can have 'read' or 'read/write' access to shared folder, but the default setting is for 'Everyone' to have 'Full Control' of a shared folder. When a folder is shared with 'Everyone, Full Control' setting on the share it is said to be 'Open' and is vulnerable to hackers and viruses. Also data contained in the folders can be modified/deleted by all users on the network. **Observation:** The folders listed below are shared with Full control to EVERYONE. • Antivirus on ASER1 - (Extranet Application Server) • VBS2 on EDB2 - (NB Database) **Impact:** *The folders are open*	Identified inappropriate share permissions should be withdrawn immediately.	

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
	to unintended access and changes which could result in loss of confidentiality/modification/deletion of data.		
2.4	**NTP not configured on servers** **Background:** Successful audit of a large network can depend on synchronization of the various logs and records maintained for the hosts on that network. Accurate time is important for the integrity of such audit logs and NTP is the standard Internet protocol for time synchronization, and it is used on most large operational networks. Because having accurate time can be important for security, especially for intrusion and forensic analysis, NTP should be used to synchronize all the devices and hosts on a network. **Observation:** Time synchronization with NTP (Network Time Protocol) server is not configured on the following servers • MARC - (SPD Application)	The clocks of all relevant information processing systems within an organization or security domain should be synchronized with an agreed accurate time source.	

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
	• IMAN - (RND Application) • BKPSERVER - (xyz Application) • SR1_DR - (Fail Over SR1) • SR2_DR - (Fail Over SR2) • SR3_DR - (Fail Over SR3) • SR4_DR - (ERP DB Fail Over) • CL01 - (Finance Payroll Application) • CL02 - (A Application) • CL03 - (B Application) • SR1 - (Database server A) • SR2 - (Database server B) • SR3 - (Database server C) • CL01_DR - (Fail Over CL01) • CL02_DR - (Fail Over CL02) • CL03_DR - (Fail Over CL03) • CL04_DR - (ERP Application Fail Over) • QA02 - (ERP QA DB) **Impact:** *Integrity of the audit logs and administrative changes may not be*		

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
	established. Further investigation of attacks to computers depends on checking the logs in different machines. The inconsistency of the time recorded by each machine makes this work and monitoring difficult.		
2.5	**Logon / Legal Notice not configured** **Background:** The notice informs the user at the time of logging about the repercussions of unauthorized access and is something like "This system is the property of XXX. Use of this system constitutes acceptance of XXX policy and consent to monitoring. Unauthorized use of this system may subject you to criminal prosecution and penalties. By logging on to these systems you are confirming that you are authorized to use these systems. If you are not authorized to use these systems or do not agree to comply with this use, do not proceed." **Observation:** Business use notice, a deterrent and warning for	Business use notice should be enabled on identified servers.	

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
	unauthorized access, 'when one logs in as administrator' is not enabled on following servers. • MARC - (SPD Application) • IMAN - (RND Application) • BKPSERVER - (ABC Application) • SR1_DR - (Fail Over SR1) • SR2_DR - (Fail Over SR2) • SR3_DR - (Fail Over SR3) • SR4_DR - (ERP DB Fail Over) • CL01 - (Finance Payroll Application) • CL02 - (A Application) • CL03 – (B Application) • SR1 - (Database server A) • SR2 - (Database server B) • SR3 - (Database server Material & Spares) • CL01_DR - (Fail Over CL01) • CL02_DR - (Fail Over CL02) • CL03_DR - (Fail Over CL03)		

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
	- CL04_DR - (ERP Application Fail Over) - QA02 – (ERP QA DB) **Impact:** *Unauthorized changes may happen and it may not be possible to initiate legal or disciplinary proceedings against unauthorized user.*		
2.6	**Inconsistent audit log configurations** **Background:** Event logs contain information about hardware and software problems and about security events on a computer. A computer running Microsoft Windows records events in three kinds of logs: application, system, and security. Event logs are used for auditing/troubleshooting or investigating past disruptions/unauthorized access. Therefore log file size and their retention period should be configured in such a manner so that log can be reviewed before they get overwritten. **Observation:** **There seems to be no basis for defining /**	Consistent audit log policy should be applied across servers and logs should be promptly backed up and manually cleared to obviate the need for overwriting. Wherever required, log size may be suitably increased.	

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
	enabling audit logs a) Audit log policy is not consistent across servers in terms of event logging, log file size and retention period. b) Audit logs configurations on all servers allow overwriting on reaching of defined maximum log size. **Impact:** *Audit trails may not be available when required. Fixing of accountability for network access/modification including administrative access/modification may be rendered difficult.*		
2.7	**Vulnerable service used for performing administrative activities** **Background:** TELNET is an Internet protocol and service that allows a user to connect to a remote computer. TELNET allows a user at one site to interact with a remote timesharing system at another site as if the user's terminal was connected directly to the remote computer. To have access to that computer, the user must authenticate to the system with a valid username and	SSH (Secure Shell) that transmits information in encrypted form should be used instead of TELNET.	

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
	password. With TELNET the information that is transferred over the network is not encrypted. It is transmitted in clear text. Anybody with a packet sniffer on the network or on a remote machine can view the information as it is exchanged, even password information. **Observation:** TELNET service is used for accessing and performing administrative activities on all UNIX servers. **Impact:** *Sniffing may reveal username and password when they are traveling in clear text. This increases the possibility of unauthorized access and subsequent unauthorized changes.*		

E: Observations and Impact – 3.0 L-3 SWITCH / ROUTERS

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
3.1	**Mutiple IOS versions in use** **Background:** The newer versions are either patched up for known vulnerabilities or such	IOS versions should be standardized across XXXXX.	

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
	services have been shutdown by default where as in older versions they still exist or not shut by default. They need to be explicitly shut down in older versions. **Observation:** Various versions of IOS (Network device operating system) as listed below are in use. - 10.2 - 11.1 - 12.2 - 12.3 **Impact:** *Maintenance may be rendered difficult because of the fact that in some cases vulnerable services are shut by default whereas in other cases they need to be shut down explicitly. Further, the chances of vulnerable services left open are more thereby exposing the network to compromise and unauthorized changes.*		
3.2	**Inappropriate configurations for password encryption** **Observation:** Password encryption (enable secret) that stores the strong and complex encrypted form	Enable password encryptions (enable secret) on the identified devices.	

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
	of password in the device is not enabled on following devices. Some of these devices, however, use weak encryption (enable password) as listed in the next point. The weak encryption is easily breakable. • Internet Router VSNL1 • XXXXXX-HO RIL Router • HO-XXXXXX RIL Router • TULIP Router XXXXX End • TULIP Router XXXXX End alteon • TULIP Router Location XYZ • TULIP Router Location XYZ alteon • Reliance Router Location XYZ • Reliance Router Location XYZ alteon **Impact:** *With the present configuration, password is stored in unencrypted form in some devices and with weak encryption in other devices. The weak encryption is also easily breakable. There is a possibility of it getting revealed by other means and chances of unauthorised access to devices are*		

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
	enhanced.		
3.3	**Weak encryption used for password storage** **Observation:** Enable password that stores the password with weak encryption is enabled on following devices. Weak encryption is easily breakable and hence the passwords may be leaked. Internet Router VSNL1 Internet Router VSNL2 XXXXXX-HO RIL Router HO-XXXXXX RIL Router HO-XXXXXX TATA Router XXXXXX-HO TATA Router TULIP Router XXXXX End TULIP Router XXXXX End alteon TULIP Router Location XYZ TULIP Router Location XYZ alteon Reliance Router	Use only enable secret and then 'no enable password' for securing the passwords.	

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
	Location XYZ Reliance Router Location XYZ alteon XXXXXX-YYYYY IPLC 512kbps router **Impact:** *These passwords can be decrypted without much difficulty and can be used to gain unauthorised access to these devices. The unauthorized configuration changes in the devices may bring down the network completely.*		
3.4	**AAA (Authentication, Authorisation and Accounting) not in use** **Background:** Authentication answers the question Who is logging in? Authorization answers the question What is this person authorized to do? Accounting answer the question What did this person do? AAA server is used for authenticating the users, allowing them access to the devices as per pre defined level of authorisation and log their activities that can subsequently be used for auditing purposes.	AAA should be configured and put in place.	

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
	Observation: AAA (Authentication, Authorisation and Accounting) server is not configured on any of the devices. **Impact:** *Investigation of the unauthorized access to these devices may not be possible as no logs will be available for this purpose. In absence of such information auditing and monitoring may also be rendered difficult.*		
3.5	**Loopback interface not in use** **Background:** When the device initiates a network connection, that connection must have some source address; typically a device will select a source address from one of the addresses bound to one of its physical network interfaces. This can be problematic in several ways, mainly because different services may not use same interface address. In addition to physical interfaces, Cisco IOS devices have the ability to define internal virtual (logical) interfaces, called	Loopback interface should be defined and configured for usage.	

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
	loopback interfaces. A loopback is a virtual interface that is always up. It is considered best practice, in configuring Cisco devices, to define one loopback interface, and designate it as the source interface for most traffic generated by the device itself. Adopting this practice yields several benefits for the overall stability and security management of a network, because the address of the loopback interface is fixed. Also, the loopback interface's address does not appear in any route-based network maps; hiding administrative aspects of the network from potential attackers. **Observation:** Loopback interface is not configured on any of the device. **Impact:** *Maintenance may be rendered difficult as the logging host may log different source addresses for the same device (having Multiple interfaces). Also administrative aspects (IP addresses) of the network*		

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
	may not be hidden from potential attackers and compromising the device and ultimately the network may become easier.		
3.6	**Missing device interface descriptions** **Background:** Documenting information such as this ensures that reconstructing configurations and diagnosing problems are made considerably easier. Providing interface description is a good practice that helps the administrators in maintenance. **Observation:** The description of device interfaces is missing in almost all router configurations. **Impact:** *The maintenance staff may have to spend time to find the use to which the interface has been put to and that may result in delays in performing maintenance activities and that ultimately will affect the availability of the device and network.*	Interface description of each of the used interfaces should be provided.	
3.7	**Administrative user not setup** **Background:**	Administrative users be configured and strong passwords	

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
	These routers are used for connecting networks at various locations to XXXXXX data centre. Their names suggest their locations. These devices are remotely managed. The administrator logs in maintenance mode and maintains their configurations. The present configurations are such that when the administrator will try to log into these routers they will not prompt for a username. They will ask for just a password. **Observation:** Administrative user is not setup on following routers. • Internet Router VSNL2 • XXXXXX-HO RIL Router • HO-XXXXXX RIL Router • XXXXXX-HO TATA Router • TULIP Router XXXXX End • TULIP Router XXXXX End alteon • Reliance Router XXXXX End • Reliance Router XXXXX End alteon • TULIP Router Location	with complexity should be used for access to these devices.	

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
	XYZ - TULIP Router Location XYZ alteon - Reliance Router Location XYZ - Reliance Router Location XYZ alteon **Impact:** *In the absence of administrative user, getting unauthorised access to these devices is rendered easier. Further auditing and monitoring of logon activity may not be possible.*		
3.8	**Missing management VLAN** **Background:** These switches are used for creating VLANs (network zones) for restricting/limiting access of different users to resources in different VLANs. A management VLAN is configured to restrict the management of L3 switches to a select few within management VLAN. **Observation:** Management VLAN (Virtual Local Area Network) is not configured on core (L3 – Layer 3) switches. **Impact:** *VLAN management can be performed from any node thereby exposing the*	A separate VLAN for management should be configured and used for VLAN management.	

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
	VLAN to unauthorized access and subsequent unauthorized changes in configurations. Unauthorized changes in VLAN configurations may jeopardise accesses of authorized user to authorized resources and therefore availability of the network may be at risk.		
3.9	**Vulnerable services not stopped** **Background:** Cisco routers support a large number of network services. Some of these services can be restricted or disabled, improving security without degrading the operational use of the router. Some of these services allow users and host processes to connect to the router. Others are automatic processes and settings intended to support legacy or specialized configurations but which are detrimental to security. General security practice for routers should be to support only traffic and protocols the network needs; the services listed above are not needed. Turning off a network service	Device configurations may be reviewed thoroughly and identified and any other unwanted service should be disabled.	

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
	on the router itself does not prevent it from supporting a network where that protocol is employed. For example, a router may support a network where the bootp protocol is employed, but some other host is acting as the bootp server. In this case, the router's bootp server should be disabled. **Observation:** Vulnerable services e.g. PAD, ip source routing, IP mask reply, ip redirects, ip bootp server etc are not disabled on any of the devices. **A list of such services, their description and recommendations is attached as annexure-I.** **Impact:** *Devices may be vulnerable to attacks and the result could vary from performance degradation to non availability of the device.*		
3.10	**Ingress and egress filtering not configured** **Background:** A packet filter allows or denies traffic based on addresses and protocols and provides control of the data transfer between networks. Most	Ingress and egress filtering should be configured.	

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
	routers can filter traffic on the basis of source IP address and destination IP address. Packet filters are especially important when they act as the gateway between trusted (private) and untrusted (public) networks i.e. Internet routers. Filters are also important for their ability to enforce addressing constraints. For example, the Internet router should ensure that packets sent from the internal or protected network must bear a source address within the range allowed for internal network addresses. This is sometimes called *egress filtering*. Similarly, the Internet router should ensure that packets arriving from the Internet must bear a source address outside the range valid for the protected (inside or private) network. This is a form of *ingress filtering*. This type of filtration can, therefore, help stop spoofing (impersonation) attacks from Internet or within the network. **Observation:** Ingress and egress filtering is not configured on devices		

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
	listed below. • Internet Router VSNL1 • Internet Router VSNL2 **Impact:** *Possibility of spoofing attack. Such attack may either degrade the performance of the device or make it completely unavailable thereby stopping Internet access completely.*		
3.11	**Undesirable ports left open** **Background:** The IP address gives a unique number for reaching someone on the Internet, just as a telephone number allows one to reach a specific destination on the public telephone network. Many larger organizations set up their telephone networks to use phone extensions. These extensions are typically 2-5 digit numbers that identify an individual phone within the organization. But from the outside, all of these extensions are associated with a single telephone number. Network port number functions similarly to a telephone extension. Taken together with a network address, a port number identifies both a computer and	Router configuration hardening practices should be documented and practiced. Periodical review of router configurations should be undertaken.	

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
	also a "channel" within that computer where network communication will take place. Just as different organizations may use the same extension numbers "inside" their primary phone number, different computers use the same set of port numbers. Alternatively we can say that every ip address is divided into ports. IP Addresses are divided into ports, so that one IP address can be used by multiple programs to send and receive data at the same time. Ports make it possible for us to check our email and browse the web at the same time. This is possible because browsing the web uses port 80, and getting email uses port 110. We can think of a port as a path for data. When a program is using a port to send or receive data, it can be thought of as being busy / not available / blocked. Meaning that no other program can use a port when it is already in use by a program. Services running on devices have logical port associations e.g. web service uses port 80, outing mail uses port 25, FTP		

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
	(file transfer protocol) uses port 21 etc by default and can be used to gather information about the protected network or weaknesses associated with these services can be exploited against the protected network. The best practice is that if a service is not running or used on a device the port associated with it is closed explicitly. **Observation:** Undesirable ports (logical ports) are left open and need to be closed on the border routers. An indicative partial list of ports, that if not used should be closed, is given below. • 1 (TCP & UDP) • 9 (TCP & UDP) • 11 (TCP) • 13 (TCP & UDP) • 15 (TCP) • 19 (TCP & UDP) • 37 (TCP & UDP) • 43 (TCP) **Detailed list of such ports is given in annexure-sheet (ports).** **Impact:** *Possibility of leakage of information about the network and subsequent*		

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
	attack. Such attack may either degrade the performance of the device or make it completely unavailable.		
3.12	**Orphaned (broken) connections permitted in routers** **Background:** TCP (Transmission Control Protocol) connections from other devices. A device may have its connection abruptly severed from the router such that the initiating device process is unable to tell the network to close the connection properly. Such a session that remains open on the router side after the client has disconnected is called an orphaned connection. One common cause of orphaned sessions arises when a client device loses power unexpectedly, or is powered off without performing a proper shutdown. Orphaned sessions can also occur due to a hung application that never completely terminates, resulting in a dead connection. A mis-configured router does not know that the connection is dead and	Include 'service tcp-keep-alive-in' and 'service tcp-keep-alive-out' commands for configuring the router.	

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
	continues to report the action as active and keeps the session open and continues to wait for a command from the client. Open sessions take up one of network connections. The maximum number of connections is limited; therefore, orphaned sessions may prevent other devices from connecting. Typically, a more important issue is that open sessions use server resources and may have locks. These locks may block other connections from performing useful work, and can sometimes be the result of a major "pile up" of locks. In severe cases, it can have device stopped working. **Observation:** The present configuration of all the routers allows orphaned (broken) **Impact:** *Broken and hanging connections may result in performance degradation and availability of the device may be at risk.*		
3.13	**SYN attack not blocked** **Background:** A SYN flood / attack is a form of denial-of-service_attack in which an attacker sends a	Include **'**ip tcp intercept list nnn' commands for configuring the router.	

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
	succession of spoofed / fake SYN requests to a target's system. The target sends a SYN/ACK (acknowledgement) in response and waits for an ACK (final acknowledgement) to come back from the initiator to complete the session set up. Since the source address was fake, the acknowledgement part of SYN/ACK never reaches the initiator and hence the response never comes back, filling the victim's memory buffers / connection queue so that it can no longer accept legitimate session requests, thereby denying service to legitimate TCP users. **Observation:** SYN (Synchronization) attack is possible with the present configuration of Internet routers. **Impact:** *SYN flood may result in performance degradation and availability of the device may be at risk.*		
3.14	**Web based administration in use** **Background:** While the web access features are fairly rudimentary on most Cisco router IOS releases,	Disable HTTP access on the identified router and instead use SSH/SSH1 access.	

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
	they are a viable mechanism for monitoring, configuring, and attacking a router. Web client used for making HTTP connection to a device stores username and passwords in cache memory. This password is retrievable from cache memory later. Further, the authentication protocol used for HTTP is equivalent to sending a clear text password across the network. **Observation:** Web-based remote administration using the HTTP protocol is enabled on HO-XXXXXX TATA Router. **Impact:** *Username and password can be obtained from cache and finally used for obtaining unauthorized access that may lead to unauthorized changes in configurations. This may put availability of device and hence network at risk.*		
3.15	**Syslog recording not in use** **Background:** Network devices can send their log messages to a centralizing syslog server that can improve the manageability of any size network and can decrease response times to	Syslog should be configured, logs regularly reviewed and record of such checking and action taken, if any, be maintained.	

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
	resolve problems. Sending log messages to a remote server also allows longer archiving of messages than in a device's limited storage. Messages stored by syslog have permanence where same is not the case when stored by device itself. When a device is power reset messages in its log are erased **Observation:** Syslog recording is not configured on any of the devices. **Impact:** *Logs may not be available when required and monitoring may be rendered difficult.*		
3.16	**SNMP Misconfiguration** **Background:** SNMP (Simple Network Management Protocol) is very widely used for router monitoring, and frequently for network device configuration changes as well. There are currently three versions of SNMP: SNMPv1, SNMPv2c and SNMPv3. IOS version 11.3 supports SNMPv1 and SNMPv2c. IOS versions 12.0 and later support all three versions of SNMP. Version 1 of the SNMP protocol, that is	SNMP should be appropriately configured and default SNMP community strings should be changed.	

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
	in use at XXXXX, is inherently very weak and uses a very weak authentication scheme based on a "community string," which amounts to a fixed password transmitted over the network without encryption. The protocol supports a connection between two entities that communicate with each other: the manager and the managed entity, the agent. The network device like router is the agent. A software application on a PC or workstation normally acts as the manager. An SNMP agent device maintains information and makes it accessible to managers. SNMP may be used to query the status of or set the values of network components in the agent. To get information from agents the manager uses passwords called community strings. There are two types of community strings in use. One is called RO (Read only) for getting information and the other is RW (Read/Write) for making configuration changes using SNMP. The default values for RO string is “PUBLIC” and for RW string is		

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
	"PRIVATE". SNMP protocol allows access restrictions to be applied by way of using access control lists for getting information from agent or making configuration changes in agent. SNMP may also be used by an entity on the network to send alerts / traps indicating problems. This facility allows devices to be monitored as part of an overall SNMP-based network management infrastructure. **Observation:** a) SNMP is not neither configured nor explicitly disabled on HO-XXXXXX RIL router b) SNMP RO (read only) community string value is left to its publicly known default value in all devices. c) SNMP RW (Read / Write) community string is left to its default value in XXXXXX-HO TATA router. d) No SNMP traps are configured for: Internet Router VSNL2 HO-XXXXXX TATA Router XXXXXX-HO TATA Router		

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
	e) SNMP traps for 'TTY' only are configured in Internet Router VSNL2. No standardization for configuring traps has been followed in others. f) SNMP access list not defined for any of the devices. Access list is used to limit machine access to the device. g) SNMP version 1 is in use and that has the weakest security. **Impact:** *SNMP can be used to obtain device configuration information that may be used to obtain unauthorized access and perform unauthorized changes to the device configurations.* *The current configuration enhances the possibility of unauthorized changes to the device configuration by use of publicly known RW (Read / Write) string.* *In the absence of access list SNMP access to the device is unrestricted and that increases the possibility of unauthorized access to configuration information and subsequent unauthorized changes.* *SNMP version 1 that is*		

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
	currently in use uses a community string for authentication purposes. Community string names are transmitted in clear text. Any attacker sniffing the network can ascertain the community name from passing traffic. Once this community string is known, the attacker can then potentially read values off of the managed device or make configuration changes.		
3.17	**Default console port configurations in use** **Background:** A Cisco router's console port is the most important port on the device. Password recovery on the router can only be done using the console port. The console port allows a hard break signal that interrupts the boot sequence of the router. If a break sequence is issued on a router within 60 seconds of the reboot, it gives complete access to the user issuing this command. The device allows displaying a banner that informs the user at the time of logging about the repercussions of possible unauthorized access.	Appropriate username / password should be setup and timeout should be configured.	

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
	Observation: a) Management (console) port default username / password settings are not changed on all the devices. b) Timeouts are left to their default values on all devices except the following devices where they have been configured never to timeout. • Internet Router VSNL1 • HO-XXXXXX TATA Router c) Management (console) port security banner is not setup on any of the devices. **Impact:** *Console port access will not require any authentication and that increases the possibility of unauthorized access and subsequent unauthorized changes to the device configurations.* *In the absence of missing banner even possibility of inadvertent access increases so also the possibility of unauthorized changes.*		
3.18	**Auxiliary ports not disabled** **Background:** Auxiliary ports are used for remote dial in access for maintenance. A modem can	Auxiliary ports should be shut down.	

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
	be connected to the auxiliary port for remote administration via dial-up. Permitting direct dial-in to any vital piece of network infrastructure is potentially very risky, and should be set up only when timely access by other means is not feasible. In general, the auxiliary port should be disabled. **Observation:** Auxiliary ports are not disabled on any of the devices and their username / password settings are left to default values except in case of Internet Router VSNL2. **Impact:** *Access will not require any authentication and that increases the possibility of unauthorized access and subsequent unauthorized changes to the device configurations.*		
3.19	**Misconfiguration in VTY access** **Background:** VTY ports are used for remote administration of network devices. By default CISCO devices support Multiple VTYs for administration and the number is more than the actual number of required	Redundant ports should be shut down. Set strong passwords for the identified devices. Apply access list for VTY access for controlled access. Log on to further	

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
	ports. Also by default no passwords are assigned to these TELNET or VTY lines. There is built-in security on the VTY lines that mandates the use of passwords to access the router via a TELNET session and therefore passwords must be assigned to access the device through VTY port. The password should be fairly complex so that it is not easily guessable. An inherent weakness of TELNET that is in use to access the devices is that TELNET transmits and receives all data in clear text, even the passwords. The device further provides for use of access control lists to limit the access to the device through these ports to a select few. By default the device also provides for connecting further to another network device from the current device however this can be restricted by properly configuring the device. **Observation:** a) Multiple VTY (Virtual terminal) ports are in use on all routers. b) Access list are not used for VTY access on any of the	devices from VTY should be disabled.	

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
	devices. c) Log on to further devices from VTY is not disabled on any of the devices. d) A very easy to guess password is used for VTY access for the following devices • XXXXXX-HO RIL Router • HO-XXXXXX RIL Router • TULIP Router XXXXX End • TULIP Router XXXXX End alteon • Reliance Router XXXXX End • Reliance Router XXXXX End alteon • TULIP Router Location XYZ • TULIP Router Location XYZ alteon • Reliance Router Location XYZ • Reliance Router Location XYZ alteon **Impact:** *Multiple VTY ports increase the risk of unauthorized access and subsequent unauthorized changes to device configurations.* *Easy to guess password increases the possibility of*		

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
	guessing the password easily and therefore increases the possibility of unauthorized access and subsequent unauthorized changes. *In the absence of access list VTY access to the device is unrestricted and that increases the possibility of unauthorized access to configuration information and subsequent unauthorized changes.* *Once an attacker has gained telnet access via a VTY, they can establish further telnet sessions from the device to other devices. It may be difficult to track an attacker in such event as the attacker may jump from one device to another device. Further it increases the possibility of unauthorized access to other devices if one device is compromised.* *The unauthorized changes in the configuration may bring down the device and eventually the network.*		
3.20	**NTP not configured** **Background:** Accurate time is important for good audit and management. Network devices support the	NTP should be configured on identified devices.	

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
	standard time synchronization protocol, NTP to keep their time-of-day clocks accurate and in synchrony. Time Logging is a critical part of network security; good logs can help find configuration errors, understand past intrusions, troubleshoot service disruptions, and react to probes and scans of network. **Observation:** NTP (Network Time Protocol) is not configured on any of the devices except XXXXXX-YYYYY IPLC 512kbps router. **Impact:** *Monitoring may be rendered difficult as time synchronization may not happen and the logs may not be that effective to find configuration errors, trouble shoot service disruptions etc..*		
3.30	**Weak protocol in use** **Observation:** TELNET which transmits data in clear text is in use for remote management of all the devices. **Impact:** *Telnet transmits everything in clear text and sniffing may reveal username and password when they are traveling in clear text. This*	Secured communication protocol like SSH should be used for remote maintenance.	

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
	increases the possibility of unauthorized access and subsequent unauthorized changes.		
3.31	**Redundant routes in use in routers** **Background:** Routes in routing table are responsible for providing information for a packet movement. It directs which route a packet should take to reach a particular destination. Routing table should contain only valid routes. **Observation:** The following are redundant routes in the routing tables 'ip route 0.0.0.0 0.0.0.0 BRI1/1 30' in Internet Router VSNL1 'ip route 0.0.0.0 0.0.0.0 BRI1/0 40' in Internet Router VSNL1 'ip route 10.5.2.0 255.255.255.0 10.101.2.2' in HO-XXXXXX TATA Router **Impact:** *Redundant routes are always a hindrance in maintenance activities that and render them difficult.*	Redundant routes should be removed.	
3.32	**Web based administration in use** **Background:**	Prefer using SSH that has not been configured on the	

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
	Web client used for making HTTP connection to a device stores username and passwords in cache memory. This password is retrievable from cache memory later. Further, the authentication protocol used for HTTP is equivalent to sending a clear text password across the network. **Observation:** Web based management of core switches is in use. **Impact:** *Username and password can be obtained from cache and used for obtaining unauthorized access. Once the access is obtained the configuration changes may be done to bring down the network.*	switches.	

E: Observations and Impact – 4.0 FIREWALL

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
4.1	**Weak protocol in use** **Background:** As a best practice is always recommended that access for maintenance should be allowed from minimum	Possibly SSH access to firewall should be used and that too should be restrictive.	

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
	possible machines. **Observation:** TELNET access to the firewall is configured with no access restrictions. **Impact:** *No access restrictions may increases the possibility of unauthorized access and subsequent unauthorized changes to firewall configurations. The unauthorized changes may even bring down the firewall and hence the network.*		
4.2	**NTP not configured** **Background:** Accurate time is important for good audit and management. Network devices support the standard time synchronization protocol, NTP to keep their time-of-day clocks accurate and in synchrony. Time Logging is a critical part of network security; good logs can help find configuration errors, understand past intrusions, troubleshoot service disruptions, and react to probes and scans of network. **Observation:** NTP is not configured.	NTP should be configured.	

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
	Impact: *Monitoring may be rendered difficult as time synchronization may not happen and the logs may not be that effective to find configuration errors, trouble shoot service disruptions etc..*		
4.3	**Inappropriate event log configurations** **Background:** Logs are used for auditing, troubleshooting past disruptions or investigations. Log size and review periods should be so set such that space is always available for writing so that they can be reviewed before they get overwritten. The settings appear to be prima-facie low. **Observation:** Log file event log size is 2000 entries and life time is 20 days. **Impact:** *Logs may get overwritten before they get reviewed and backed up.*	Log file parameters should be reviewed for their appropriateness and if required reset.	
4.4	**ICMP not blocked** **Background:** ICMP is designed for sending control and test messages across IP networks. The two most important ICMP	ICMP requests should be dropped.	

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
	messages are Echo Request (8) and Echo Reply (0). Echo Request and Echo Reply are utilized by the \`ping\` command to test network connectivity. With echo packets an attacker can create a map of the sub networks and hosts (devices / machines) behind the device. Also, he can perform a denial of service attack by flooding the device with echo packets. **Observation:** ICMP (Internet Control Message Protocol) Echo and reply are not blocked. **Impact:** *Possibility of DOS attack that may put availability at risk.*		
4.5	**Weak encryption for confidentiality used in VPN** **Background:** ESP is used to provide confidentiality, data origin authentication, connectionless integrity, an anti-replay service (a form of partial sequence integrity), and limited traffic flow confidentiality. The firewall is configured to encrypt and accept encrypted packets (traffic) using DES algorithm	Encryption using 3DES should be used.	

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
	that uses 56 bit key for encryption to provide for confidentiality of the data during transit. DES is considered very weak these days because of availability of high computing power at very nominal cost that may be used for cracking the key. **Observation:** ESP (Encapsulating Security Payload) – DES (Data Encryption Standard) with SHA (Secure Hash Algorithm) is allowed. ESP–DES with MD5 (Message Digest ver 5) is allowed. **Impact:** *Weak encryption algorithms in use may reveal the encrypted information to an attacker who might subsequently use this information to further compromise the network.*		
4.6	**Weak encryption for authentication used in VPN** **Background:** Diffee-Hellman algorithm is used for public-private key encryption and that in turn is used for identification and authentication of the sender. The minimum length of the key that is considered safe	Use at least Group 2 that provides 1024 bits of keying strength.	

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
	and recommended as per good practice is 1024. **Observation:** Diffee-Hellman group-1 that provides for 768 bits of keying strength and is the weakest of all is also allowed. **Impact:** *Weak encryption algorithms in use may reveal the encrypted information to an attacker who might subsequently use this information to further compromise the network.*		
4.7	**Redundant object groups in use** **Background:** Object groups are created to group various objects into one and a meaningful name is given to such groups so that by knowing the group name the administrator can understand the nature of the objects contained in the group. **Observation:** Object groups 'Dealer' and 'NB' are redundant and not in use. **Impact:** *Unused objects can create confusion for the*	Redundant object groups should be removed.	

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
	administration performing the maintenance activities that and therefore may render maintenance difficult		
4.8	**Password management not configured.** **Background:** Password management is used for defining the periodicity at which the password must be changed. Password change at periodic intervals reduces the risk of password compromise. **Observation:** Password management is disabled. **Impact:** *Disabled password management increases the risk of password compromise and that renders unauthorized access and subsequent unauthorized configuration change easier.*	Password management should be enabled with suitable management configurations.	
4.9	**High firewall idle time out.** **Background:** Idle timeout is used to logout the user/administrator when there is no activity on the device for the specified amount of time. **Observation:**	Idle timeout value should be reviewed and suitably reduced.	

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
	Firewall idle time out value is set to 15 minutes. That is prima-facie high. **Impact:** *Longer idle time outs increase the possibility of unauthorized access as logged in device may remain unattended.*		
4.10	**Ant spoofing not enabled** **Background:** Spoofing or impersonation is used for hiding the identity of the real attacker. The attacker may use some forged source IP address for sending the attack packets. The anti spoofing feature contains details of some known forged addresses and if configured in the device will not let packets carrying these forged addresses to pass through it. **Observation:** Anti spoofing feature of the firewall is not enabled. **Impact:** *Availability of device and hence network may be at risk and it may be difficult to identify the attacker in case of need.*	Feature should be enabled.	
4.11	**Redundant / inappropriate**	Identified	

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
	firewall rule configurations **Background:** Firewall rules are configurations in firewall that are deployed for filtration of traffic by the firewall. These rules either allow or deny traffic based on predetermined criteria and the criteria are made as per security needs of the organization. **Observation:** a) Following rules are redundant. • Slot 1 interface1 – Policy 1 • Slot 2 interface1 – Policy 1 and Policy 3 b) In rule 6 of slot 2 interface1 specific ports are not defined rather all ports are permitted. Also IP ranges permitted are too permissive (21 class C subnets i.e. 21x254 hosts). c) Rule 7 of slot 2 interface1 provides for a very large port range and that is too permissive. d) Rule 9 of slot 2 interface1 provides for redundant	redundant rules should be removed and other identified rules should be suitably amended.	

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
	destination IPs. • 192.168.4.x • 192.168.4.0 **Impact:** *Possibility of unauthorized access to the firewall that may result in unauthorized changes that may affect the availability of the network. Maintenance may also be rendered difficult.*		

E: Observations and Impact – 5.0 LOGICAL ACCESS CONTROLS

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
5.1	**Large number of administrators configured for domain administration** **Background:** The Enterprise Administrators are most privileged users in windows active directory system and are empowered to add, modify and remove users, active directory / group policy objects, reset passwords etc. for an entire domain.	Number should be pruned to bare minimum.	

Sr. No	**Observation & Impact**	**Recommendation**	**Auditee Response & Implementation Timeline**
	The Domain Administrators are next most privileged users after Enterprise Administrators in windows active directory system and are empowered to add, modify and remove users, group policy objects, reset passwords etc. for an entire domain. **Observation:** a) There are 7 users who are member of Enterprise Admins group. b) There are 13 users who are member of Domain Admins group The number are prima-facie too high. **Impact:** *This may lead to* u*nintended access/unauthorized modification to active directory architecture i.e. the access rights of the users may be unauthorizedly changed*		
5.2	**Inappropriate password configurations** **Background:** Periodic change of password is a good security practice that reduces the chances of password getting	All accounts other than application login accounts should be subjected to periodic password	

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
	compromised. **Observation:** 52 users including privileged users are not required to change their passwords periodically. **Impact:** *Never changed passwords increase the chances of password compromise and that in turn increases the chances of unauthorized access and risk to confidentiality and integrity of data.*		
5.3	**Generic users in existence** **Observation:** 102 user accounts (not identifiable by username) appear to be generic and being used by more than one individual. **Impact:** *Fixing of individual accountability may be rendered difficult incase of unauthorized access/modification of network resource.*	All user accounts should be identifiable with specific individual.	
5.4	**Large number of disabled / expired users in existence** **Observation:** 1014 disabled user accounts and 47 expired user accounts exist. **Impact:** *Disabled or expired*	Disabled / expired accounts should be reviewed and deleted	

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
	users are always a risk for unauthorized access as they may get activated even unintentionally. Also user maintenance/ reconciliation may be rendered difficult.		
5.5	**Large number of users never logged in** **Observation:** 173 users never logged on to the system. **Impact:** *Never logged users credentials are more vulnerable to be used to gain unauthorized access/use of network resource.*	The accounts should be reviewed and if not required disabled/deleted.	
5.6	**Test users in existence** **Observation:** 6 test users are in existence. **Impact:** *Test user's credentials are more vulnerable to get compromised to gain unauthorized access/use of network resource.*	Test users should be reviewed and if not required disabled/deleted.	
5.7	**Inappropriate settings for unlocking locked users** **Observation:** User accounts locked due to unsuccessful login attempts are automatically unlocked after 10 minutes. Configured auto unlock time appears to be prima-facie too low.	There should be no automatic unlocking of accounts. Instead such account should be unlocked only by administrator.	

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
	Impact: *Automatic unlocking users locked due to defined unsuccessful login attempts are more vulnerable to attack for user name/password guessing specifically when configured time is low.*		
5.8	**Build in administrator account not renamed** **Background:** Local build in administrator accounts are created when an operating system is installed on the server. The user name of these accounts is publicly known. So they are always a security risk, if they are not renamed. Security best practice suggest renaming of these accounts. **Observation:** Local build in administrator accounts have not been renamed on any server including domain controller. **Impact:** *Default user name may render usage of this account easier. This account is a privileged account with full powers and therefore has access to all resources including data. The data is therefore exposed to the risk of loss of confidentiality and*	Local build in administrator should be renamed on all servers.	

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
	integrity.		
5.9	**Redundant Group Policy Objects in existence** **Background:** Group Policy Object Objects are used for defining and grouping various security configurations to be enforced at a group level. This group level could be an organizational unit or even a domain. **Observation:** Redundant Group Policy Object like New Group Policy and New Group Policy 1 with no policy defined are existed. **Impact:** *Identified redundant group policy object may supersede the domain policy if enforced on any organization unit and this may lead to unauthorized access to network and active directory maintenance may be rendered difficult.*	Redundant group policy objected should be removed.	
5.10	**Inappropriate last log on settings** **Background:** Good security practice suggests that last user name should not be displayed to the logging user. **Observation:**	The option should be enabled.	

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
	Do not display last user name is not enabled on any server. **Impact:** *Displayed last username renders unauthorized access as unauthorized user easier as the user truing to log in is not required to guess the user name to get the access.*		
5.13	**Inappropriate password policy** **Background:** Password policy allows for setting of a minimum password length, its complexity, age, history, periodicity of change etc so that guessing of password by unauthorized persons is rendered difficult. • ASER! - (Extranet Application Server) • MARC - (SPD Application) • IMAN - (RND Application) • BKPSERVER - (LEGATO Application) • SR1_DR - (Fail Over SR1) • SR2_DR - (Fail Over SR2) • SR3_DR - (Fail Over	Password policy should be enabled on identified servers.	

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
	SR3) • SR4_DR - (ERP DB Fail Over) • CL01 - (Finance Payroll Application) • CL02 - (A Application) • CL03 - (B Application) • SR1 -(Database server A) • SR2 -(Database server B) • SR3 - (Database server C) • CL01_DR - (Fail Over CL01) • CL02_DR - (Fail Over CL02) • CL03_DR - (Fail Over CL03) • CL04_DR - (ERP Application Fail Over) • QA02 - (ERP QA DB) **Observation:** Password policy (which defines the password age, length, complexity and history) is not enabled on following servers. **Impact:** *Servers with weak or no password policy are more vulnerable to easier guessing of password and subsequent unauthorized access.*		

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
	Therefore, the confidentiality and integrity of the data may be at risk.		
5.14	**Oracle default passwords not changed** **Background:** Software / packages come with various default username and passwords for initial usage that are publicly known. Such passwords should be changed immediately after installation of the systems. **Observation:** Oracle default passwords for privileged access are not changed on SR4_PR (Production database server for Application A) and QA02 (Production database mirror server). **Impact:** *Publicly known default user name and password may be used for unauthorized system access and changes.*	Default passwords should be changed immediately.	

E: Observations and Impact – 6.0 INTERNET AND ANTIVIRUS CONTROLS

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
6.1	**Internet access available on servers** **Background:** Machines with Internet access are always more vulnerable to malicious attack than the ones not having such an access. Security best practices suggest that Internet access should be made available freely on all servers. **Observation:** Internet access is enabled on all servers. **Impact:** *Internet access from server zone can lead to threats of malicious code attack from Internet.*	Internet access should be disabled on all servers in trust zone.	
6.2	**Inconsistent antivirus updates** **Observation:** a) Although virus/antispam/IWSS updates are scheduled to be pulled automatically from respective websites but failure alerts for such updates are not configured. b) Antivirus updation on servers is not through push mechanism. Updation is done manually and therefore generally not consistent.	Update failure alerts may be configured. Push mechanism should be used for updation on servers.	

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
	Impact: *May result in virus and malicious code attack to internal server zone which intern can result to non-availability of network/network resources*		

E: Observations and Impact – 7.0 EMAIL

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
7.1	**Inappropriate password policy for mobile devices access for mail** **Observation:** Email synchronization to mobile devices is configured in MS-Exchange server with weak password configurations like minimum length 4 characters and without any complexity etc. **Impact:** *Weak passwords are more vulnerable to get compromised hence may lead to unauthorized access.*	Password configuration should be suitably strengthened.	

E: Observations and Impact –8.0 BASIC HYGIENCE

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline

8.1	**Low basic hygiene index for desktops** **Observation:** On a sample of 10 desktops allowed for basic hygiene check following were observed: • On 3 desktops the virus definitions were dated back to January 2006 • On 7 other desktops they were 4 days old. • Floppy/CD ROM drive/USB storage devices were enabled on all desktops. • OS patch updatation was 3 months old. • Vulnerable services were not disabled on any desktop.	It is be ensured that virus definitions are regularly updated on all systems. Usage of Floppy/CD ROM drive/USB storage devices should be restricted in line with security policy. OS patches should be regularly updated. Undesirable vulnerable services should be stopped.	

E: Observations and Impact –9.0 BACKUP

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
9.1	**Backup strategy not geared up to ensure zero data loss** **Background:** Zero data loss is availability of complete transaction data for applications in the event of system failure / disk crashes. Environments where there are large number of transactions in very short times and this data	Backup strategy should be reviewed and geared up to ensure zero data loss at least for critical applications.	

Sr. No	Observation & Impact	Recommendation	Auditee Response & Implementation Timeline
	is critical, it is a good practice to have backup strategy geared up for zero data loss. **Observation:** Backup strategy is not geared up to ensure zero data loss of critical applications in the event of disaster. **Impact:** *Could result in non availability of critical application in the event of disaster.*		
9.2	**Backup not up to date** **Observation:** File server "LOCATION 1" is not backed up from 5th December 9999 as per the backup policy. **Impact:** *Could result in non availability of critical data in the event of disaster.*	Identified server should be backed up as per the policy.	

A Guide to Forensic Audit Report

Introduction

Globally the financial and corporate fraternity has suffered the impact of many scams such asEnron, WorldCom, Xerox, Satyam scam,Ketan Parekh securities scam, Speak Asia scam, Saradha chit fund scam, etc. In all these cases, though the modus operandi was different yet the motive in all these scams indicated manipulation in financial statement. Widespread rise in the cases of financial accounting manipulation is being reported in the coming years. The Indian Companies Act also recognized the frauds as a risk and it made mandatory for the statutory auditors to report in their auditors report. Recently Companies (Auditor's Report) Order, was revised in 2016 and it requires auditors to report, amongst others, *"whether any fraud by the company or any fraud on the Company by its officers or employees has been noticed or reported during the year; If yes, the nature and the amount involved is to be indicated."*It has been observed that majority of the corporate frauds and scams are the outcome of manipulation of accounts and accounting window dressingdesigned to deceive others for wrongful gains with intent to cause wrongful loss to the company and its shareholders. In this backdrop, the techniques of forensic auditing have gained importance.

Forensic auditing, which is based on the practices of forensic accounting is the best possible course of action for reducing financial manipulations and malfeasance in today's scenario. The questions about the ability of applying the forensic audit techniques to provide reasonable financial oversight and the broader acceptance of principles-based accounting methods have the potential to create a new approach to risk assurance. Forensic auditing requires variety of duties, jobs and skills depending on whether one is in law enforcement, litigation, intelligence, etc. The auditing technique in each category may differ but despite the differences there are skills and duties that are encompassed in all of them. One such centralized duty is drafting forensic reports. Drafting reports or just communicating findings in general, is essential to the forensic audit field. The very best examination/Investigation/audit/review is purposeless if it cannot be intelligently conveyed.

What is Forensic Auditing?

The term has not been defined in regulatory guidance. However, in simple language it refers to the specific guidance carried out in order to produce evidence. Forensic Audit task involves an investigation into the financial affairs of the entity and is often associated with investigation into the alleged fraudulent activity. The object of forensic auditing is to relate the findings of audit by examining and gathering legally tenable evidence and producing it to the Court. In the process the corporate veil is lifted in case of corporate entities to identify the fraud and the persons responsible for it. Forensic auditing involves application of audit skills to legally determine whether fraud has actually occurred. The entire process includes planning, gathering evidence, reviewing the evidence and reporting of the same. In the process it aims at naming the person(s) involved in the fraud with a view to take legal action.

Meaning of Forensic Reports?

One of the forensic auditors' primary function is the dispersal of the forensic process to the person(s) for whom it's intended. To be successful at this job they must write forensic reports that are technically accurate, unambiguous and easy to construe. Forensic reports provide findings and recommendations as a result of the forensic related investigation. It details the cause and consequences of any instance, detect the occurrence of any criminal activity, illegal act or potential fraudulent activities. The scope of forensic reports is to furnish a written and factual basis on all the discovered abnormal financial activities, whether past or present and to identify the names of the person(s) involved with a view to take future action. Forensic reports are used to provide scientific testimony that either proves or disproves the argument in a case. One can resort to forensic reports as evidence for the purpose of future litigation. Therefore, utmost care and caution is necessary while drafting the report.

Relevance of Forensic Reports

A forensic report is the end result of the forensic auditor. The forensic report has the potential to influence the legal outcome. The forensic reports prepared by the forensic auditor provide conclusive answers to the questions like who, what, where, why and how. Forensic reports play a major role in keeping the organization clean and transparent. These reports go a long way in impacting the operation of the organization and preparation of its financial reports in accordance with the rules and regulations as prescribed by the concerned authority. These reports find relevance for several purposes including detection of criminal activity, illegal acts, and potential fraudulent activity or civil liabilities, admissible as evidence, as proof of what was found or not found, etc. Forensic reports provides stronger and relevant forensic evidence to address the specific case issues that have been raised. It presents further forensic information in a definite format that is relevant and specific to the case concerned. The forensic reports also helps prompt earlier guilty pleas and can strengthen the prosecution or defence case by assuring that any further evidence is purpose-built. Moreover, it adds value by dealing with the specific needs of the case. In each of the above mentioned circumstances, and so many more, the forensic reports have a significant and immediate impact on the subject of the evaluation. For the cognition of this impact the forensic auditors must take greater care in writing the report.

Engagement Letters

The engagement letter is the written contract between the practitioner, the client(s), the attorney, the attorney's client and possible other parties. The engagement letters is used to establish an understanding of the services to be performed and the work involved. It primarily defines the responsibilities of each party to the agreement. It is a source to document the understanding of the parties pertaining to the scope of work involved, the objectives to be attained, the parameters to be considered, the rights and duties of the practitioner and that of the client, context within which engagement is to be considered, etc. The practitioners who provide forensic accounting and litigation services ordinarily use engagement letters. Such engagement letters contains the following clauses:

1. Introductory Information: Date, Address and Case Name
2. Scope of Work involved and agreed by the management
   - (i) Objectives
   - (ii) Parameters to be considered
   - (iii) Relevant timelines
   - (iv) Reporting expectations
   - (v) Understanding of facts and circumstances
   - (vi) Context within which engagement is to be conducted
   - (vii) Whether you can provide expert witness service
   - (viii) Whether the scope can be expanded/customized as the work progresses or not.
3. Independence and Conflict of Interest
4. Description of Practitioner Services

5. Description of Professional Team
6. Acknowledgement by client
7. Professional Fee and other expenses and manner of invoicing
8. Performance by Client
9. Representations by the Client towards the documents/ information to be provided
10. External Information
11. Work-paper and literature
12. Benefit of advice
13. Communication/mode of communication
14. Indemnity clause
15. Privacy, Ownership, and Use of Materials
16. Non-disclosure by client of the advice/report
17. Confidentiality clause
18. Dispute resolution provisions
19. Limitations on liability and damages
20. Termination/ expiration of the engagement
21. Force Majeure Clause
22. Governing Laws and Jurisdiction

Some of the essential clauses are discussed below:

1. **Scope of Work involved and agreed by the management**: This clause defines the work to be done and identifies the client. The role of the management is also described in this clause. This clause also explains the objectives and parameters to be considered, the context within which the engagement is to be conducted, whether the scope can be expanded as the work progresses or not. The clause provides the management's responsibility to make all financial records and related information available to the accountant/auditor in a timely manner.
2. **Indemnity Clause**:Indemnity clause defines and assigns the risk of carrying out transactions between two parties by obligating one party to bear the expenses incurred by the other party under certain circumstances.The scope of the indemnity clause depends on the

nature of engagement and the local/state governing laws that apply. One should be careful while adding an indemnity clause and must include a clear dispute resolution provision. It is on occasion when the parties disagree over an indemnity claim that the clear dispute resolution provision will come into play. However, limits on the liability are important. Much deliberation has to put to whether to exclude indemnity obligations from a disclaimer of consequential damages.

3. **Non-disclosure by client of the advice/report:** An auditor's paper works and the various documentation carried out in the process of audit are the property of the auditor. To avoid future conflict with the client there should be a clear non-disclosure clause by client of the advice/report detailing that the client promises to not make any disclosure of any of the pertinent fact and make every diligent effort to maintain confidentiality. Moreover, apart from maintaining confidentiality it should also document the client's promise to immediately advise the auditor if it becomes aware of any inaccuracy in its record-keeping or dishonesty in any of its business dealings.

4. **Dispute Resolution Provisions:** There should be a dispute resolution clause allowing the parties to decide upon mechanism/procedure for the resolving the dispute before the dispute actually arises. Alternative dispute resolution procedures like arbitration, negotiation, mediation may be beneficial for timely resolving the disputes between parties and reducing litigation costs. These are alternative method for having a dispute decided outside the formal court room setting.

5. **Termination/Expiration of the Engagement:** Every engagement letter should elaborate the circumstances in which each party may terminate or withdraw from the engagement. This clause should explain that circumstances may arise which prevent completion of the engagement or may require the auditor to withdraw from the engagement. It is always beneficial to use broad language allowing both the client and the auditor to terminate the engagement at any time and for any reason subject to any rules and regulations of professional conduct that may apply to the auditor.

Drafting of Forensic Audit Report

Report writing is essential to the forensic audit field. The very best audit is useless if it cannot be intelligently conveyed. The basic principles of good report writing are that it should be both technically accurate and easy to read. Reports that are both concise and precise are the best. While drafting the report the information collected or the findings are generally broken into few different categories, such as an overview; executive summary including the facts in brief, methodology in brief, findings in brief; background and allegations; detailed methodology, main report, procedure performed, findings in detail, limitations, disclaimers, etc. It is always useful to structure the report in Headings to differentiate data and make the report more reader friendly.Regardless of the type of structure or length of the report, the conclusion is the most important part. Forensic reports have the tendency to significantly impact and influence the outcome of the case. Therefore care should be taken to only include relevant and reliable data. The report should accurately lay out the details of an incident. The structure of the forensic report should be as given below:

Structure of Forensic Report

1. Index
2. Overview
3. Executive summary
   i. Facts in brief
   ii. Methodology in brief
   iii. Findings in brief
4. Background and Allegations
5. Detailed Methodology
6. Main Report
7. Detailed Time-line
8. Scope reconciliation
9. Detailed methodology- collection of evidence and implementation
10. Procedure Performed
11. Findings in detail-point wise finding and analysis
12. Limitations
13. Disclaimers
14. Glossary and Abbreviations
15. Appendices and Exhibits

Few of the basic principles of drafting a good forensic report are:

- The report should be understandable to the decision-makers and easy to read by the intended audience.

- The report should be unambiguous; language should be clear and should not be open to misrepresentation.
- References should be easily given to the relevant facts of the incident.
- The report should offer valid conclusions, opinions, and recommendations when needed.
- It is recommended to always keep on updating the report in the process of examination and investigation. It can be done by writing down relevant information through each step or preparing notes.
- Use confidentiality language whenever appropriate. The word “Draft” in a header or footer should be used before the report is final.
- Knowledge of interpretation of rules is advisable such as *Ejusdem generis*("of the same kinds, class, or nature"), *Noscitur a sociis*("a word is known by the company it keeps"), etc.
- Reports tend to get lengthy and are often very specific and detailed. Therefore it is always advisable to break up the structure for ease of understanding.
- State the complete facts of the case including the names of the persons involved, amount involved, complete details of the issue.
- The details of the evidences essential to prove the entire issue has to be detailed.
- The choice of words and the usage of language should be simple. Avoid using technical/legal jargons or flowery language. The choice of word is crucial and has a legal impact.
- The observations should be supported with Annexures and other Evidences as exhibits.

From the above discussion it can be concluded that forensic audit report is made for a particular purpose i.e. it must be acceptable to the court. Every attempt should be made by the forensic auditor to include relevant information while excluding the irrelevant and immaterial data and information. The forensic audit report must be prepared in a manner that it is able to convey the meaning it seeks to as per the scope of the forensic audit. As indicated above, the forensic audit report must be clear and unambiguous and should be duly supported by relevant evidence and document.

INDEX

	Promoters of this Company and details of their respective shareholding and directorships.	
15.	**Annexure – 3** Details of such dubious transactions on which no concrete findings could be achieved.	
16.	**Annexure – 4** Certified copies of financial statements of the Company for the last 10 financial years, as obtained from the office of Registrar of Companies.	
17.	**Annexure – 5** The statements of Mr. Faulty as recorded by the team.	
18.	**Annexure – 6** The vouchers and bank statements / documents received from various banks in respect of transfers made from May, 1994 to August, 1999.	
19.	**Annexure – 7** The certified copies of land records obtained from the patwaris of various taluks in Bangalore, Delhi and Chandigarh	
20.	**Annexure – 8** the certified copies of the documents obtained from the Sub-Registrar's offices of the concerned districts of Bangalore, Chandigarh and Delhi.	
21.	**Annexure – 9** The copies of formal complaints filed by depositors as obtained from various courts.	
22.	**Annexure – 10** The records provided by the Company in respect of the depositors of the Company.	

For GRT Advisors and Consultants
Grt Advisor
Director

Date:

Place: New Delhi

Sample Information Systems Audit & Forensic Audit Report

1. OVERVIEW

The present assignment was handed over to GRT Advisors and Consultants to conduct the forensic audit of Con Limited as there were various allegations against the company for misappropriation and siphoning of funds of the company and diversion of assets.

The engagement letter was executed on 25th August, 2015, as per which the scope of forensic audit was defined to be as under:

a. Analyses of all relevant documents including the secretarial, accounting and administrative documents in respect of the Company and its group and subsidiaries companies;

b. Extracting data and collecting documents from all the concerned third parties including government / statutory authorities and banks;

c. Interviews of management, staff and employees, and other relevant third parties; and

d. Preparation of Report.

2. EXECUTIVE SUMMARY

2.1 Facts in Brief

The Department of Police, NCT had approached *GRT Advisors and Consultants* for conducting a forensic audit of the company being Con Limited (in short the “Company”) which is a public limited company incorporated on 15th November, 1988 under the provisions of the Companies Act, 1956.

As per the information available to the Department of Police, the Company had launched various public deposit schemes such as recurring deposit scheme, fixed deposit and cash certificate. The total amount of public deposits accepted by the Company amounts to Rs. 298.09 crores. However, only 0.01% of the above amount has been invested by the company in statutory liquidity ratio. Further, upon a preliminary examination conducted by the Department of Police, it was observed that the entire group of companies is in financial trouble and repayment of interest and principal to depositors. It was also observed that various complaints including civil and criminal complaints, complaints before statutory agencies such as EOW and RBI and various winding-up cases have been filed against the different group companies and their directors / promoters primarily alleging fraudulent diversion of money and dishonest misappropriation of funds.

Under these circumstances, an Engagement Letter was signed between *GRT*

Advisors and Consultants and the Chief of Department of Police on 25thAugust, 2015 for conducting the forensic audit of the Company.

2.2 Methodology in brief

It was decided and agreed by our team to follow a detailed methodology for conducting the investigation for the purposes of forensic audit of the Company. The said methodology consisted of the following broad steps:

a. Procurement of documents from the Company and its group / subsidiary companies (if any);

b. Procurement of documents from necessary third parties;

c. Interviewing and recording the statement of the management of the Company, including ex-management and also employees and staffs of the Company;

d. Interviewing and recording the statement ofnecessary third parties;

e. Detailed analyses of all necessary documents and evidence on record; and

f. Preparation of Report.

2.3 Findings in brief

Upon a detailed investigation, it has been found that the Company and its directors are liable for prosecution under various provisions of the Indian Penal Code, 1860, Companies Act, 2013 and any other relevant laws on the following three accounts:

a. Siphoning and misappropriation of Funds of the Company to the tune of Rs. 103.45 crores by acquiring immovable properties at Bangalore, Delhi and Chandigarh;

b. Cheating and fraud and siphoning of money of the Company may be lodged against the Company and its directors for siphoning of money of the Company in the garb of deposit schemes being floated by the Company; and

c. Non-maintenance of the statutory records of the Company as well as its group and subsidiary companies

3. BACKGROUND

3.1 Con Limited (in short the “Company”) is a public limited company incorporated on 15th November, 1988 under the provisions of the Companies Act, 1956 vide Registration No. 87-091345 having its registered office at Con Bhawan, UGF, Banke Road, Delhi – 110056. The Company was listed on the Bombay Stock Exchange (BSE) from 1994 to 2007 after which it was delisted by the BSE.

3.2 The Company was granted Certificate of Commencement of Business on 16th December, 1988.

3.3 The Company was promoted by 3 promoter directors being as under:

3.3.1 Mr. XYZ

3.3.2 Mrs. JHG

3.3.3 Mr. TYR

Later, various other directors were inducted on the Board of Directors of the Company, and a detailed list of Board of Directors since inception of the Company is attached hereto as **Annexure – 1**.

3.4 The main objects of the Company is as under:

"To promote the formation and mobilization of capital and to promote industrial finance by way of advance, deposit of lending money, to manage capital, savings and investment, to act as a discount and acceptance house and purchase.

To carry on and undertake business of finance and trading out, finance, re-finance, to act as or carry on the business of consultants, advisers, experts and technical collaborators in matters pertaining to, without prejudice to the generality of the foregoing, portfolio management services, syndication of loans, counselling and tie-up for project and working capital, infrastructure finance, corporate re-structuring, corporate planning & strategic planning, foreign currency lending or borrowing, project planning and feasibility, investment counseling, setting up of joint ventures and further perform any other kind of role as an Intermediary or Advisor in the Securities Market."

3.5 Subsidiary Companies: The Company has one Company being Frauds Private Limited which is a wholly owned subsidiary of the Company. Further, Conmaker Private Limited is the subsidiary of Frauds Private Limited, and in effect is a step-down subsidiary of the Company i.e. Con Limited.

3.6 Promoter Group Companies: The Promoters of the Company had also promoted various other companies for the purpose of its objects and for making investments in other verticals. The various other companies promoted by the Promoters of this Company and details of their respective shareholding and directorships has been detailed and marked hereto as **Annexure – 2**.

3.7 As per the information made available, the Company had launched various public deposit schemes such as recurring deposit scheme, fixed deposit and cash certificate. The total amount of public deposits accepted by the Company amounts to Rs. 298.09 crores. However, only 0.01% of the above amount has been invested by the company in statutory liquidity ratio. Also, it appears that the Company has failed to comply with almost all the norms necessary for non-banking financial companies.

3.8 Upon a preliminary examination conducted by the Department of Police, it was observed that the entire group of companies is in financial trouble and repayment of interest and principal to depositors. It was also observed that various complaints including civil and criminal complaints, complaints before statutory agencies such as EOW and RBI and various winding-up cases have been filed against the different group companies and their directors / promoters primarily alleging fraudulent diversion of money and dishonest misappropriation of funds. The above cases are pending trial before the competent courts of law having necessary jurisdiction.

3.9 Under these circumstances, it was felt necessary to conduct a forensic audit of the Company and the team of the undersigned were appointed vide Engagement Letter dated 21.04.2015.

4. ALLEGATIONS

The various allegations against the Company and its directors, which also form part of the scope of the present audit, are as under:

4.1 Diversion and dishonest misappropriation of funds to the tune of Rs. 103.45 crores including acquisition of immovable properties at Bangalore, Chandigarh and Delhi.

4.2 Failure on the part of the Company and its other group companies and/or subsidiary companies in repayment of deposits accepted by them.

4.3 Non-maintenance of books of accounts and statutory records.

5. DETAILED METHODOLOGY

5.1 The team was deputed to investigate into the affairs of the Company and all its group / subsidiary companies since incorporation and to analyse the financials of the said companies.

5.2 Understanding the quantum of work and to facilitate a comprehensive report, the team was divided into threegroups who were assigned specific areas of work.

5.3 One group was specifically responsible for scrutinizing and analyzing the documents and records available with the Company and its group/subsidiary companies. The team/group members scrutinized various secretarial, accounting and administrative records of the companies which included financial statements of the said companies, statutory records being maintained, ledger accounts, vouchers, registers, bank statements and all other relevant documents being in the custody of the companies. However, considering the fact that the companywas quite old, most of the secretarial, accounting and administrative records were hampered and most of the documents were not maintained by the Company in its requisite form.

5.4 Second group was sent to the third parties including Registrar of Companies, Banks were the accounts of the companies were maintained, Police and EOW Department to investigate into the affairs of the said companies.

5.5 Third group was deputed to interview the relevant persons including the management of the said companies and third parties to confirm and verify the team's understanding of the entire assignment.

5.6 The step-wise actions taken by the team for conducting the present audit are as under:

5.6.1 As a first step, all the secretarial, accounting and administrative records of the said companies including the books of accounts and statutory records were inspected by the team and photocopies of all the necessary documents were taken into custody by the team. The companies were specifically requested to provide access to the said documents/records including the records of the group and subsidiary companies. The team made personal visits to the premises of the Company, group companies and subsidiaries at their registered offices as well as all other corporate offices, and went through the voluminous records and books of accounts stored therein. However, since the company appeared to be quite old, thus all the documents could not be made available to the team officials.

5.6.2 It was also observed during the investigation that the Company had accepted deposits from approximately 33,20,198 small depositors through cash payments and not a single investor/depositor had made the payment on non-cash basis or through cheque or any other mode of payment. The details of all the investors / depositors as provided by the Company were also taken. It may be worthwhile to mention here that the Company and its officials were very reluctant at the first instance to provide the exact details of such investors / depositors to the team members. However, upon a lot of persistence and enquiry, the Company provided uncollated and unorganized data of all the depositors and considering the limited timeline of the entire assignment, the team could not spend much time and effort on the said document and thus a detailed finding could not be reached as regards the said data. However, it may be advisable to depute someoneto analyse the said data at a minute level.

5.6.3 The companies were having bank accounts with various banks across the country. However, it was observed that a large number of bank accounts were maintained by these companies in unrelated states i.e. states where no registered / corporate / regional offices of the companies were present. It was also observed that only a few accounts maintained by the Company were in the Public Sector Banks. Further, the Company also had few accounts in non-scheduled banks. The major banks with whom the Company and its group / subsidiary companies had important accounts are as under:

i. A Bank, Delhi

ii. B Bank, Chennai

iii. C Bank, Puducherry

iv. D Bank, Assam

v. E Bank, Bombay

vi. F Bank, Link Road, Tirunevelli

vii. G Bank, Chandigarh

Certified copies of statement of accounts in respect of the accounts maintained by the Company were sought from all the banks where the said companies had even a single bank account. Accordingly, the team obtained the said certified copies of statement of accounts along with photocopies of all relevant documents including account opening forms, payment/receipt vouchers etc. However, various transactional vouchers could not be made available to the team since the said vouchers were destroyed by the banks in terms of the rules for preservation of records.

5.6.4 Certified copies of the records available with the Registrar of Companies regarding authorized capital, issued capital, changes in directorships, annual accounts etc. were also obtained.

5.6.5 The members of the team also went to all the places where immoveable properties of the companies were situated. The team also went to the offices of patwaris, tehsildars and Sub-Registrars of the area and collected the relevant documents / details in relation to the said properties of the companies.

5.6.6 Various litigations are also pending against the companies and accordingly the relevant documents pertaining to the same were also collected by the team.

5.6.7 Thereafter, the team interviewed the management (present and ex-management), staffs and employees and all other relevant parties associated with the companies. Further, the team also contacted and interviewed third parties associated with the companies including the depositors, officials of the banks, dealers etc. The management, especially the ex-management were reluctant to reply to all the questions being asked by the team and most of the replies given by the management could not also be corroborated with the documents made available to the team since the concerned transactions were old and proper records were not maintained.

5.7 Upon completing a thorough exercise as detailed above, the present report has been prepared by the team in view of the specific allegations. However, due to various constraints as explained above, a lot of transaction which prima facie appeared to be dubious could not be investigated by the team in a proper manner and the team could not reach on proper conclusions in respect of the same. Details of such dubious transactions on which no concrete findings could be achieved are enlisted as **Annexure – 3** to this Report.

6. METHODOLOGY VERIFICATION

6.1 The team initially carried desk-based analyses and reviews of the records and documents available to the team and categorized the details into various broad transactions.

6.2 After the first round of review and analyses, the transactions were also verified on the basis of information obtained from the third parties. Further, to gain a better understanding of various transactions and to validate various assumptions arising out of the initial desk-based review, the team was deputed for actual field visits.

6.3 Various transactions were also corroborated by way of the statements recorded during the interviews.

6.4 Thereafter, when the team found that documentary evidence supporting various transactions was incomplete, the team undertook an indepth analyses of the said transactions. The in-depth analyses included field visits, verification of authenticity of documents / records with records held by third parties and also roles and responsibilities of each managerial persons (including ex-management), staff and employees were determined transaction-wise. Further, at various places opinions from Experts including handwriting experts have also been taken to verify the authenticity of various documents.

6.5 However, wherever the team could not determine the authenticity of documents / record in relation to any transaction and / or the team could not collect necessary documentary evidence, such transactions have been marked as inconclusive

7. DETAILED TIME-LINE

7.1. As per the engagement letter, the entire assignment was to be completed within a period of 10 months. The time lines for the said assignment are as under:

(a) 25th August, 2015–Date of execution of engagement letter;

(b) 28th August, 2015 – Deputation of team for the purposes of forensic audit.

(c) 30th August – 25th September, 2015 – Inspection and procurement of statutory records of the Company and its subsidiaries and group companies.

(d) 26th September – 13th November, 2015 – Inspection and procurement of documents from third parties.

(e) 14th November, 2015 – 15th December, 2016 – Initial scrutiny and desk-review of all the documents obtained.

(f) 16th December, 2015 – 29th March, 2016 – Interviews of all relevant persons, management, employees and staffs of the Company as well as relevant third parties, and recording of statement on oath.

(g) 30th March, 2016 – 15th May, 2016 – Detailed, in-depth analyses of the allegations and corroboration of the same with the documents and statements on record.

(h) 16th May, 2016 – 08th June, 2016 – Preparation of the Report.

8. SCOPE RECONCILIATION

8.1. Based on the initial meeting with the Department of Police, the scope of the forensic audit of the Company was to look into the three broad allegations, being (a) Diversion and dishonest misappropriation of funds to the tune of Rs. 103.45 crores including acquisition of immovable properties at Bangalore, Chandigarh and Delhi; (b) Failure on the part of the Company and its other group companies and/or subsidiary companies in repayment of deposits accepted by them; and (c) Non-maintenance of books of accounts and statutory records.

8.2. For looking into the above said allegations, a detailed analysis of all the secretarial, accounting and administrative documents of the Company and its group and subsidiary companies was required. Also, analyses of all the documents obtained from third parties were also required.

8.3. In addition to the above, detailed interviews were also required to be conducted to extract relevant information.

8.4. Accordingly, as per the tasks performed by the team in the past 6 months, the scope reconciliation of the present assignment is as under:

S.No.	Scope	Status	Remarks
1.	Analyses of all relevant documents including the secretarial, accounting and administrative documents in respect of the Company and its group and subsidiaries companies.	Completed	Certain aspects could not be checked since the Company was quite old and the earlier records were not properly maintained by the Company. Also, the management were initially reluctant in giving all the details of

			the depositors. Later an unorganized data was given which was taking considerably huge amount of time for extracting relevant information for the purposes of the Report. Thus, various transactions could not be checked minutely.
2.	Extracting data and collecting documents from all the concerned third parties including government / statutory authorities and banks.	Completed	Certain transactional vouchers could not be made available by the Banks since the said vouchers were destroyed by the Banks in terms of the rules for preservation of records.
3.	Analyses of all documents extracted from the third parties	Completed	Since certain documents could not be made available to the team thus certain transactions which prima facie seemed to be fraudulent could not be analysed in detail.
4.	Interviews of management, staff and employees, and other relevant third parties	Completed	Completed and detailed transcript also prepared.

9. MAIN REPORT

9.1. Brief of the Company

9.1.1. Con Limited i.e the “Company” is a public limited company incorporated on 15th November, 1988 under the provisions of the Companies Act, 1956 vide Registration No. 87-091345 having its registered office at Con Bhawan, UGF, Banke Road, Delhi – 110056.

9.1.2. The Company's original registered office was at RT-1, Block 2, Sector 3, Delhi and was later shifted to Con Bhawan, UGF, Banke Road, Delhi – 110056 on 27.09.1997.

9.1.3. The Company was listed on the Bombay Stock Exchange (BSE) from 1994 to 2007 after which it was delisted by the BSE.

9.1.4. The Company was granted Certificate of Commencement of Business on 16th December, 1988.

9.2. Main objects of the Company

9.2.1. The main objects of the Company is as under:

"To promote the formation and mobilization of capital and to promote industrial finance by way of advance, deposit of lending money, to manage capital, savings and investment, to act as a discount and acceptance house and purchase.

To carry on and undertake business of finance and trading out, finance, re-finance, to act as or carry on the business of consultants, advisers, experts and technical collaborators in matters pertaining to, without prejudice to the generality of the foregoing, portfolio management services, syndication of loans, counseling and tie-up for project and working capital, infrastructure finance, corporate re-structuring, corporate planning & strategic planning, foreign currency lending or borrowing, project planning and feasibility, investment counseling, setting up of joint ventures and further perform any other kind of role as an Intermediary or Advisor in the Securities Market."

9.3. Details of Management of the Company

9.3.1. As per the various documents received from the office of Registrar of Companies, the details of management for the past 10 years are as under:

S.No.	**Name and last known address**	**Designation**	**Date of Appointment**	**Date of Cessation**
1.	Mr. XYZ [*Address*]	Promoter Director	15.11.1988	Continuing
2.	Mrs. JHG [*Address*]	Promoter Director	15.11.1988	Continuing
3.	Mr. TYR [*Address*]	Promoter Director	15.11.1988	Continuing
4.	Mr. AHKJ	Additional Director	19.04.1997	29.03.2007
5.	Mrs. NBF	Director	20.09.1994	11.08.2008
6.	Mr. P.K. JHD	Director	21.01.1999	04.01.2016
7.	Mr. BHG	Director	01.05.2000	08.03.2007

A detailed list of Board of Directors since inception of the Company is already attached hereto as *Annexure – 1*.

9.4. **Financial Position of the Company**

9.4.1. The Net worth of the Company for the financial year ending on 31st March, 2016 was Rs. 189.03 crores. The extracts of Balance Sheet and Profit and Loss Account for the financial year ending on 31st March, 2016 is reproduced herein below:

[***Tip:*** *The details of B/s and P/L account as per latest audited balance sheet be reproduced for the sake of ready reference.*

Also, figures / extracts from any other financial statement may also be reproduced wherever necessary for corroborating the same with the allegations as well as the findings]

9.5. Certified copies of financial statements of the Company for the last 10 financial years, as obtained from the office of Registrar of Companies is annexed hereto as **Annexure – 4**.

9.6. Upon a preliminary examination conducted by the Department of Police, it was observed that the entire group of companies is in financial trouble and repayment of interest and principal to depositors. It was also observed that various complaints including civil and criminal complaints, complaints before statutory agencies such as EOW and RBI and various winding-up cases have been filed against the different group companies and their directors / promoters primarily alleging fraudulent diversion of money and dishonest misappropriation of funds. The above cases are pending trial before the competent courts of law having necessary jurisdiction.

Allegations in brief

9.7. Diversion and dishonest misappropriation of funds to the tune of Rs. 103.45 crores including acquisition of immovable properties at Bangalore, Chandigarh and Delhi.

9.8. Failure on the part of the Company and its other group companies and/or subsidiary companies in repayment of deposits accepted by them.

9.9. Non-maintenance of books of accounts and statutory records.

10. FINDINGSIN DETAIL – POINT-WISE FINDING AND ANALYSIS

Finding No. 1: Siphoning and misappropriation of Funds of the Companyto the tune of Rs. 103.45 crores by acquiring immovable properties at Bangalore, Delhi and Chandigarh

10.1. That during investigation, it was observed that the Company had made payments to the tune of Rs. 103.45 crores to Mr. Faulty, who was a proprietor in the firm namelyFaulty Associates. However, upon verification of the records of the Company no necessary resolutions / minutes of meetings or any other statutory record was found for giving such huge amount to a third party. Upon a further investigation into the records of Faulty Associates and upon recording the statement of Mr. Faulty on oath it was ascertained that Mr. Faulty was the relative of one of the directors of the wholly-owned subsidiary of the Company. Mr. Faulty also admitted to have received the said amount. The statements of Mr. Faulty as recorded by the team are annexed hereto as **Annexure – 5**.

10.2. The said amount of Rs. 103.45 crores were transferred through RTGS mode in 17 different installments. The transfer was made through 13 different banks and the payment was completed from May, 1994 to August, 1999. However, all the vouchers in respect of the said transfers could not be obtained from the banks since the same were very old and most of them were destroyed. The vouchers and bank statements / documents received from various banks in respect of transfers made from May, 1994 to August, 1999 are collectively annexed hereto and marked as **Annexure – 6**.

10.3. Upon a prima facie review of documents available with the Company, it was observed that the Company had purchased various land parcels in Bangalore, Delhi and Chandigarh. Thereafter, the team was sent to the patwari and Sub-Registrar's office for verification of land details so purchased, whereunder all the details related to the said land parcels were obtained. It was also observed that the said parcels were brought by the same person namely Mr. CFG, on behalf of the Company under a power of attorney dated 12.12.1994. The copy of the said power of attorney was obtained from the Sub-Registrar's office and Mr. CFG was also interviewed and his statement was recorded on oath. Upon investigation, it was revealed that the power of attorney was fabricated and no authority was ever given to the said person and he did all the said transactions upon receiving instructions from Mr. XYZ, the promoter director of the Company. Also, no resolution was ever passed by the Company to acquire any of the land parcels, so acquired on behalf of the Company. The certified copies of land records obtained from the patwaris of various taluks in Bangalore, Delhi and Chandigarh are annexed hereto as **Annexure – 7** and the certified copies of the documents obtained from the Sub-Registrar's offices are annexed as **Annexure – 8**.

10.4. The team further interviewed all the promoter directors of the Company as well as directors of its group companies, and the same has revealed a various dubious transactions for which the directors are liable to be prosecuted under Sections 405, 408, 419 and 420 of the Indian Penal Code, 1860.

[***Tip:*** *The relevant sections of Indian Penal Code, 1860 may be quoted.*]

10.5. Further, Mr. Faulty and Mr. CFG are also liable to be prosecuted under Section 120B of the Indian Penal Code, 1860 for criminal conspiracy.

[***Tip:*** *The relevant sections of Indian Penal Code, 1860 may be quoted.*]

Finding No. 2: Failure on the part of the Company and its other group companies and/or subsidiary companies in repayment of deposits accepted by them

10.6. Upon investigation, it was observed that all the investors have invested in the various schemes of the Company on cash basis only, and not a single investor/depositor has made the payment on non-cash basis or through cheque or any other mode of payment. Further, the proper details of all the investors were not available with the Company, and only name and amount invested was noted in a register. No proper records were maintained by the company. Only details of few investors who had filed formal complaints with the Courts / Company Law Board were made available through public records. The copies of formal complaints filed by depositors as obtained from various courts of law are annexed hereto as **Annexure – 9**.

10.7. During the initial phases of investigation, the Company and its officials were reluctant to give any information in respect of the deposits accepted. Upon further enquiry, only minimal documents were provided to the team. Further, the team also contacted Registry of relevant courts and Company Law Board and obtained information about the depositors who had filed formal cases against the Company for repayment of deposits. The records provided by the Company in respect of the depositors of the Company are annexed hereto as **Annexure – 10**.

10.8. The team thereafter tried contacting each and every depositor whose name and phone number/ address was mentioned in the register/ record maintained by the Company. Out of 33,20,198 small depositors, only 26,005 could be contacted. Upon contacting the said depositors, the statements were recorded on oath whereunder about 21,540 depositors have stated that they have never deposited any money with the Company and most of them were not even aware of the name of the Company. The statements of depositors as recorded on oath is annexed hereto as **Annexure – 11**.

10.9. Thus, a formal case for cheating and fraud and siphoning of money of the Company may be lodged against the Company and its directors for siphoning of money of the Company in the garb of deposit schemes being floated by the Company.

Finding No. 3: Non-maintenance of books of accounts and statutory records

10.10. During the entire process of investigation, it was observed and noted by the team that most of the statutory records were not available with the Company as well as its group and subsidiary companies.

10.11. It was also noted that name of one of the group companies was struck-off from the Register of Companies maintained by RoC due to non-filing of statutory documents with the Registrar for 8 years.

10.12. In view of the prima facie opinion made as per the observations during the investigation, it is opined that the Company is liable for prosecution by the Registrar of Companies.

11. LIMITATIONS

11.1. One of the major limitations faced by the team was the time constraint. Various persons could not be interviewed due to paucity of time for the entire assignment.

11.2. Further, Company and its officials were very reluctant at the first instance to provide the exact details of such investors / depositors to the team members. However, upon a lot of persistence and enquiry, the Company provided uncollated and unorganized data of all the depositors and considering the limited timeline of the entire assignment, the team could not spend much time and effort on the said document and thus a detailed finding could not be reached as regards the said data.

11.3. The Company appeared to be quite old, thus all the documents could not be made available to the team officials.

11.4. Various transactional vouchers could not be made available to the team by the respective banks since the said vouchers were destroyed by the banks in terms of the rules for preservation of records.

11.5. The management, especially the ex-management were reluctant to reply to all the questions being asked by the team and most of the replies given by the management could not also be corroborated with the documents made available to the team since the concerned transactions were old and proper records were not maintained.

12. DISCLAIMERS

12.1. *This Report is based exclusively on the facts and circumstances described during the engagement of the team for conducting Forensic Audit and is given based on the representations, express or implied, and based on our interpretation of law, which may differ to other person. Existence of any other factual or historical background not provided to us might require a conclusion different from the one expressed herein.*

12.2. *The information contained herein is specific only to the facts of the present case and cannot be used in any other matter and is not intended to address the circumstances of any particular individual or entity other than what has been described in the Report. Although we* *have endeavoured to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate thereafter. No person should act on such information without appropriate professional advice based on the circumstances of a particular situation.*

For GRT Advisors and Consultants
Grt Advisor
Director

Date:

Place: New Delhi