Template for submitting comments/inputs on draft Test Guide titled "FRAUD MANAGEMENT AND CONTROL CENTRE (FMCC)"

(Draft Test Guide No. TEC/TS/SW/FMC-01/03 AUG 10)

Name of Manufacturer/Stakeholder:

Organisation:

Contact Details:

S. No	Clause No.	Clause	Comments	Other Remarks, if any

Note: The comments/inputs on the draft Test Guide (Draft Test Guide No. **TEC/TS/SW/FMC-01/03 AUG 10**) may be provided in the above format vide email to **director-al.tec-dot@gov.in, ddglte.tec@gov.in**

TEST SCHEDULE
AND
TEST PROCEDURES FOR
FRAUD MANAGEMENT AND CONTROL CENTRE (FMCC)

(Against TEC GR No. TEC/GR/SW/FMC-01/03 MAR 10)

No. TEC/TS/SW/FMC-01/03 AUG 10

DEPARTMENT OF TELECOMMUNICATIONS
TELECOMMUNICATION ENGINEERING CENTRE
KHURSHID LAL BHAWAN, JANPATH
NEW DELHI- 11000

INDEX

Test Schedule and Test Procedures
For
Fraud Management And Control Centre (FMCC)
(Against TEC GR No. TEC/GR/SW/FMC-01/03 MAR 10)

No. TEC/TS/SW/FMC-01/03 AUG 10

CHAPTER -1
INTRODUCTION

1.0 **Scope of testing:**

This document contains the test schedule for the equipment deployed in the National Network against GR of Fraud Management and Control Centre (FMCC).

1.0.1 The FMCC shall effectively detect, analyze and control various possible frauds presently identified and also likely to arise in future on account of introduction of new services in fixed and mobile network.

1.0.2 The FMCC shall be capable of detecting and controlling the frauds in real time as well as near-real time basis.

1.1 Tests / compliance statement for different clauses are mentioned in **'Test Cases'** . In addition to these, Vendors shall also give the compliance statement for different IETF RFCs, Protocols, APIs, 3GPP and other standards as mentioned in the relevant clauses.

1.2 Chapter – 2 gives the Hardware & Software conformity check, List of certificates to be taken and List of testers used etc.

1.3 Protocol implementation to the extent covered by the tests contained in this document will be verified as a minimum requirement.

CHAPTER -2

Conformity Checks and Certificates

1. Technical Information to be supplied by Manufacturer/Supplier

S.No.	Clause No.	Technical Information	Remarks
1.		Detailed information related to connectors, cables, details of protocols, details and formats of all types of data/messages. Availability of testing equipment,	
2.		Protocol Implementation Conformance Statement (PICS) for all the protocols used.	
3.		Comprehensive information in the form of soft and hard copies concerning the API.	

2. List of Test results/certificates to be taken

S.No.	Clause No.	Details	Remarks
1.	Chapter-5	**Qualitative Requirements (QR) :** Ensure that the supplier / manufacturer conforms to the all quality requirements as per chapter-5.	
2.	Chapter-6	**Electromagnetic Interference (EMI/EMC):** The equipment shall conform to the EMC requirements as per Chapter-6 of GR. The manufacturer / supplier shall submit a test certificate and test report from test agency. The test agency for EMI/EMC compliance shall be an accredited one and details of accreditation shall be submitted.	
3.	7.1	**Safety Requirements:** The manufacturer/ supplier shall submit a certificate in respect of compliance as of the clause	
4.	10.2.3	**Requirement specific to leap year problem:** Compliance certificate along with test results shall be taken from supplier	

5.	10.3	**Power Supply** Compliance certificate shall be taken from supplier	

3. Hardware conformity Check

A list of hardware details upto PCB level with identification shall be provided by the supplier. Verify that the hardware equipped conforms to the hardware list provided.

(i) Show rack layout, individual shelf layout and position of PCBs in each shelf. Indicate the w x d x h measurements also.

(ii) Fill up hardware details in the following tabular form:

Equipment 1:

Description	**Make**	**Model No.**	**Any other Identification**

Rack 1:

Shelf 1:

Description	**Identification**	**Quantity**

PCBs :

S. No.	**Description**	**Identification**	**Quantity**
PCB 1:			
PCB 2:			
. . . .			
PCB N:			

Shelf 2:
:
:
Shelf N:

Rack 2:
:
:
Rack N:

Equipment 2:
:
:
Equipment N:

4. Software Conformity Check

(1). List complete details regarding the software (Version, details of all modules/blocks, files, checksum etc.,) before starting the testing and verify.

S.No.	Software details	Remarks
1.		
2.		

(2). List complete details of software patches introduced during testing phase in the following format.

S.No.	Patch description	purpose	Patch Identity	Date on which patch was introduced
1.				
2.				

(3). List complete details regarding the software (Version, details of all modules/blocks, files, checksum etc.,) after completion of testing.

S.No.	Software details	Remarks
1.		
2.		
3.		

5. List of Testers to be used :

Provide a list of all testers used during testing. Fill up the details in the table given below:

S. No.	Description of Tester	Make	Model No.	Used for
1.				
2.				
3.				

CHAPTER-3

Test Cases

S.No	Clause No.	Test Case	Test	Observation	Remarks
1	**Chapter-1**	**Introduction**	**General, No Testing required.**		
	Chapter 2	**System Architecture**			
	2.1.1.1		**Remote Site Equipment** Check that the Remote site equipment contains (a) Mediation Device (MD) (b) Remote site processor (RSP) (c) Interface to WAN (d) Interface to switches, billing and commercial systems		
	2.1.1.1.1		Check that MD can retrieve CCS7 signalling messages from 2 Mbps PCM streams by means of a passive high impedance bridge isolator without causing any attenuation/loss of signalling information without altering/introducing messages/patterns in the signalling channel.		
	2.1.1.1.2		Check that MD has the capability of retrieving the information from any time slot automatically / as programmed by the user.		
	2.1.1.1.3		Check that RSP has the capability to control a number of mediation devices. It shall collect data from MD, filter the desired data, convert into CDR and transfer CDRs to the Central site through WAN.		
	2.1.1.1.4		Check the storage capacity of RSP to store the CDRs and it shall provide interface devices to backup the system data, CDRs, etc., in a Catride Tape/DAT. The RSP shall support GUI based user interface for operating the system.		
	2.1.1.1.5		The interface to the WAN shall provide necessary communication between the RSP and the Central Site.		
	2.1.1.1.6		Check that the RSP is interfaced to the switches, billing and commercial systems through appropriate interfaces, for acquisition		

			of data periodically for detecting various frauds on near-real time basis.			
	2.1.1.2		**Central Site Equipment** The Central Site Equipment shall be one and common to all the Remote Sites. It shall contain (a) Central Site Processor (CSP) (b) Multi-user Work Station (c) Interface to WAN (d) High speed line printer(s) and (e) Interface to other Central Sites (optional)			
	2.1.1.2.1		Check that the CSP communicates with the Remote Site and receive the CDR data from the RSP and analyze for detecting various frauds on real time basis.			
3	**Chapter 3**	**Functional Requirements**				
	3.1.1		Verify that the supplier has provided necessary hardware and software, mediation devices, line interfacing equipment etc as required to interconnect the FMCC to various systems for collecting the inputs.			
	3.1.3		Verify that the FMCC is capable of accepting and analyzing the inputs in different formats depending on the system to which it is interfaced.			
	3.1.4	**Switching System**				
	3.2.1	**A**	**Check that the following frauds are detected in Real Time**			
			Nature of Fraud	**Methods of detection**		
		Technical (external)	Automatic Telephone Line Isolator	Call Thresholds and profile deviation check.		
		Technical (internal)	(i) Providing STD/ISD facility with/without detailed billing	From CDR generated by FMCC and subscriber profile /		

			category to STD barred subscribers.	subscriber database.		
			(ii) Providing free terminating call category to subscriber.	From CDR generated by FMCC		
			(iii) Diversion of long distance circuits to unauthorized locations.	From CDR generated by FMCC (No CLI or CLI not mapped in FMCC)		
			(iv) PBX fraud	From CDR generated by FMCC, threshold and profile deviation check.		
		Non- Technical	(i) Clip-on Fraud	Call thresholds and profile deviation check.		
			(ii) Call forwarding / Multiple call forwarding fraud	Threshold and profile deviation check.		
			(iii) Electronic Devices Fraud	From CDR generated by FMCC		
			(iv) Call back fraud	From CDRs generated by FMCC, threshold, destination check and profile deviation check.		
			(v) Three way calling	From CDRs generated by FMCC, threshold and profile deviation check.		
			(vi) Bypassing of International traffic	From CDRs generated by FMCC, threshold, destination check and profile deviation check.		
			(vii) Premium Rate Service	Threshold and profile deviation check.		
			(viii) Mobile Frauds	Geographical / velocity check. Threshold, destination and profile deviation check.		

			Check that the following frauds are detected in Near Real Time			
			Nature of Fraud	Methods of detection		
		Technical (external)	(i) Accessing the O&M port of the switch from remote and perform opening & closing of telephones or other services	By analysis of switch Log and Advice Note from commercial centre. or By processing the billing centre / commercial centre data and the data generated by FMCC from CDRs.		
		Technical (internal)	(i) Manipulation of databases of billing, charging, routing, subscribers	Switch log and comparing OMC files with the previous day.		
			(ii) Changing the equipment number, during preparation of bulk billing tape	By analysis of Switch Log and Advice Note		
			(iii) Withdrawing the detailed billing category and suppressing detailed bill information of a subscriber	By analysis of Switch Log and Advice Note		
			(iv) Misuse of certain dangerous commands in the switches	By analysis of Switch Log and Advice Note		
			(v) Unauthorized Transiting at TAX	By analysis of System routing and charging files.		
			(vi) Fraud at billing and commercial centre.	By processing the billing centre / commercial centre data with the data generated by FMCC from CDRs.		
			(vii) Pre-paid frauds	By Analysing data from VMC and data base generated by FMCC from CDRs		
	3.3.3	**Inputs for Analysis:**				

	3.3.3.1		Check that the FMCC is generating the Call Detail Records (CDRs) from the CCS-7 signaling links on the routes viz., Inter-TAX, TAX-International Gateway exchanges, TAX to TAXs of neighboring countries, MSC,STP and Point of Interconnect with PLMN and PSTN operators		
	3.3.3.2		Check that the FMCC is able to retrieve the following information from billing system, which is used for real time detection of fraud. (i) Authorized subscribers(all relevant details). (ii) New Subscribers(all relevant details). (iii)Subscribers as per the category such as residential, commercial, govt., service, PCOs, etc., (iv) Class of service/entitlements of subscribers (v) Lines provided to trunk boards(OTD lines) (vi) List of defaulters (vii) Disconnection/reconnection lists (viii) CDRs of subscribers (ix) Fortnightly Call charge readings		
	3.3.5	**Detection and Analysis**			
	3.3.5.1		Verify that the supplier has provided a detailed explanation and flow charts for the logic of detection and analysis of fraud in real time.		
	3.3.5.2		Check that the FMCC can generate subscriber profiles of each subscriber to show specific calling behavior and destinations called, for both working days and holidays from the information collected from the billing centre and commercial centre.		
	3.3.5.3 **3.3.5.4**		Check that the FMCC updates subscriber profiles from the CDRs generated from the CCS-7 messages based on usage days defined by System Administrator (normally 10 to 30 days). Take a print of subscriber profile and record it.		
	3.3.5.5		Check that the subscriber profile contains following fields.		

			(i) Subscriber's Identity such as directory number/equipment number/account number etc. and all other relevant details (ii) Opening date and type/category etc. (iii) Average Charge per Call made during different time bands. (iv) Average Duration Per Call made during different time bands (v) Number of STD/ISD Calls made during different time bands (vi) Number of STD/ISD Calls made per day/week/month (vii) Number of STD/ISD Calls made during peak-day/Sunday/Holiday (viii) Accumulated charge of STD/ISD Calls made per day/week/month (ix) Number of long duration calls made during different time bands (x) Number of long duration calls made per day/week/month (xi) Average of premium rate call charges per day/week/month (xii) Number of premium rate calls during different time bands (xiii) Frequently called national/international destinations. (xiv) Rarely called national/international destinations. (xv) Number of incoming STD/ISD Calls per day/week/month (xvi) Number of call forwarded during different time bands (xvii) Number of call forwarded per day/week/month. Check that it is possible to add or delete a field in the subscriber profile using MMC.		
	3.3.5.6		Check that it is possible to change time bands for thresholds for various time bands as per the tariff structure for national and international calls (varies for groups of countries), which may change time to time as per the policies of Service Provider.		
	3.3.5.7		Check the generation of subscriber profile deviation alarms by making test calls.		
	3.3.5.8 **3.3.5.9**		Check that necessary tools are available to generate twenty number of Check List/ Hot list/ Black List . Some of the Check List/ Hot list/ Black List could be		

			i) New lines ii) Unauthorized lines iii) Suspected lines iv) Lines to be specially observed v) Risk/fraudulent lines vi) Fraud destinations/area codes(NSD or ISD) vii) PCOs/Payphones viii) OTD Lines ix) Low calling lines x) Medium calling lines xi) High calling lines Check that it is possible to generate/ modify/ delete the list by the System Administrator		
	3.3.5.10		Check that the FMCC supports **Exception List** to prevent generation of alarms for certain entries in the lists. Check that the entries in the exception lists are user programmable.		
	3.3.5.11		Check that th CDRs generated by the FMCC are checked against the entries in the Check List/ Hot list/ Black List and exceptional list(s) to generate alarms		
	3.3.5.12		Check that the FMCC supports Threshold Lists, which are defined for group(s) of subscribers. Check thresholds for following. a) Charge per STD/ISD Call during different time bands b) Duration per STD/ISD Call during different time bands c) Number of STD/ISD Calls during different time bands d) Number of STD/ISD Calls during normal day/peak day/Sunday/ Holiday/week/month e) Accumulated charge of STD/ISD Calls per day/week/month f) Long duration STD/ISD Call in progress (maximum duration for any call to be in progress without disconnection and an alarm shall be generated when the threshold is crossed so that appropriate action can be taken)		

			g) Charge, duration and number of premium rate service calls during different time bands and per day/week/month. h) Charge, duration and number of calls forwarded to STD/ ISD during different time bands and per day/week/month. Check that FMCC generates an alerts if any of the above threshold limit is crossed.		
	3.3.5.13		Check that FMCC provides a tool to define 'rule' to set 'Call Patterns' (Refer Clause 3.3.4.5 (ii)) (i) It should be possible to combine 'Call Patterns Rules' logically. (ii) It should be possible to define a new rule on any field of the CDR. (iii) It should be possible to modify/delete an existing rule. (iv) It should be possible to display/print of all defined rules. Take a hard copy of 'Call Patterns Rules' defined .		
	3.3.5.15		Check for 'Geography / Velocity checks' in case of Mobile Calls.		
	3.3.5.16		Check that the prioritization of the alerts can be given into frauds based on the following weighting factors. (i) Type of threshold and the no. of threshold crossings and value of call(s). (ii) Number of Destination Check alerts generated. (iii) Geography/Velocity Check (applicable for Mobile calls) (iv) Nature of fraud detected.		
	3.3.5.17		Check that the system should have a capability to compare calling information of subscriber under investigation with that of known fraudsters for confirmation of fraudulent activity. This is different from profile based detection activity and is used for confirmation (analysis) of an alarm caused by calling activity of any subscriber.		
	3.3.5.18		Check that real time frauds are generated by FMCC within 5 minutes from the arrival of condition.		

	3.3.5.19		Check that the **prioritized cases** generated by FMCC giving following details and store them for further investigation. a) case no. , b) date, c) calling subscriber number, d) name & address, e) name of the originating exchange, f) called subscriber number, g) call origination time, h) call termination time, i) call duration, j) charged units, k) suspected nature of fraud, l) counter measures suggested, etc.		
	3.4		**Near Real Time Detection**		
	3.4.3		Inputs for Analysis		
	3.4.3.1		Check that the FMCC retrieves the following databases. (i) Switching systems: a) Transaction log/OMC log b) Databases of analysis, routing, charging, subscriber Class of Service/entitlements (ii)Commercial system: Advise Notes for service provisioning		
	3.4.4		**Detection Methodology**		
	3.4.4.1		Check that the FMCC performs data integrity & audition as per following details. (i) The Transaction/OMC log, (a) Check for certain dangerous commands,		

			(b) The subscriber management commands shall be audited against a valid Advise Note or disconnection/reconnection order (ii) The data integrity of the databases of routing, analysis, charging, subscribers, etc., shall be checked with the previously collected databases and generate error lists.		
	3.4.4.2		Check that the FMCC is able to sort the log as per commands by username, type of command i.e. subscriber management, routing management, charging management, trunk group management, etc., and/or type of operation i.e. creation, modification, suppression, etc., and store in the central site		
	3.4.4.3		Check that the FMCC generates listings of analysis, routing and subscribers from the above databases and store in the central site.		
	3.4.4.4		Check that the FMCC accepts the inputs in different formats from all switches, billing and commercial centre..		
	3.4.4.5	**Fraud at billing and commercial centre**	Check that FMCC checks the data integrity of the billing information received from billing centre against the Advise Note for service provisioning received from Commercial centre. Any disparity in the billing amount shall also be checked from the data base generated from the CDRs. In case of any mismatch an alert should be generated		
	3.5		**Fraud Control & Counter Measures**		
	3.5.1		(i) Check that the system supports high level commands/ macros for carrying out subscriber management such as barring/restricting the access to STD/ISD, disabling the incoming/ outgoing access, temporary disconnection, etc., The command syntaxes are different for each type of switching system. (ii) Check that the system indicates the counter measure and the high-level commands/macro operation required for controlling a given fraud. This may include the phone no., name of the exchange and operation proposed.		

			(iii)On confirmation by the fraud investigator, Check that the system initiates a password session on the concerned switching system port, transmit the command by suitably converting the high level command to the command format that can be accepted by the switching system. (iv) Check that the system captures the responses of the switching system based on which it indicate the results.		
	3.5.2		Check the ability of system to execute on the high level commands/macros for the above operations, on demand by the fraud investigator, as per 3.4.1 (iii) and (iv).		
	3.5.3		Check that the automatic and on demand operation can be provided through password access.		
	3.6		Check that FMCC gives an audio and visual alarm or sends SMS / e-mails on detecting certain user defined high priority fraud so that an immediate action can be taken		
	3.7		Check that FMCC shall be able to update the STD/ISD/ MSC/Local Switch Code list from the CDRs generated by it.		
	3.8		Check that FMCC shall be able to update the Premium rate service numbers list from the CDRs generated by it.		
	3.9		Check that FMCC shall give audio and visual alarm if there is an error in file transfer from the switches, billing centre or commercial centre.		
	3.10		Check that whenever there is a change in area code or bulk transfer of numbers, FMCC shall provide an easy method to update the system database		
	3.11		Check the inter-linking of FMCCs of different zones for query/exchange of data for investigations.		
	3.12		Check that the FMCC monitors the status of the CCS-7 links and data flow on the interfaces to other mediation devices in real time and display the status.		

	3.13		Check that the FMCC monitor the traffic/load on each CCS-7 link and update at least once in 3 minutes and report.		
	3.14		Check that FMCC reports that how many CDRs generated, how many of them are processed and how many of them are dropped for various reasons.		
	Chapter 4	**Interconnectivity and Interoperability Requirements**			
	4.1.2	**Interface of FMCC with switching system for retrieval of office-data:** .	Verify that interface with digital switching system is provided by following means : (a) X.25 link for direct data transfer. File transfer protocol should be compatible with that used by the switching system. (b) Wherever it is not feasible to provide the X.25 link, the FMCC shall be interfaced on asynchronous RS232C port at data rates upto 9600 bps connected on 2w/4w-leased line/dial up line (c) Wherever the switch log/OMC log is not stored in the hard disk in the switching systems such as E10B, the FMCC shall provide a mediation device, which can collect and store the OMC log from the OMC on real time and transfer to the central site. The OMC port is an output port working in RS232C protocol.		
	4.2	**Interface with Billing and Commercial Systems**	(a) Check the system is capable of interfacing with the Billing and Commercial Systems in a LAN / WAN Configuration. (b) Check that the FMCC is able to interact with various systems in the language which is specific to each system without making any changes in the existing systems		
	4.3	**Wide Area Network (WAN)**	Check that the communication between the RSPs and CSP is provided through WAN. The WAN shall support 2Mbps E1 inter		

			face or ISDN PRI or single/multiples of 64 Kbps links as per the bandwidth requirements.		
	4.4		Check that the system is able to manually copy the inputs (other than CCS-7 messages) from storage medium such as floppy, Magnetic Tape, Catridge Tape and DAT tape, Optical disk etc.		
	Chapter -5	**Qualitative Requirements (QR)**			See chapter 2 clause 2 of this document
	Chapter-6	**Electromagnetic Interference**			See chapter 2 clause 2 of this document
	Chapter-9 Other mandatory Requirements				
	9.1.1	**System administration**			
	9.1.1.1		Verify that a user-friendly GUI (Graphical – User-Interface) based on 'WINDOWS environment' or any other environment is provided for easy administration of FMCC. It should support the management of databases, initialisation, interrogation, modification and deletion of subscriber-specific parameters and global parameters.		
	9.1.1.2		Man-machine language should be in English by providing English based commands and responses.		
	9.1.1.3		It should also be possible to carry out these operations by issuing commands from the remote centre.		
	9.1.1.4		Check that suitable safeguards have been provided in the man-machine communication programs to debar unauthorized persons from accessing the databases.		
	9.1.1.5		Check that access to system operations is controlled through multi-		

			level password and authentication checks.		
	9.1.1.6		Check that the man-machine language has the facility for restricting the use of certain commands or procedures to certain staff / terminals.		
	9.1.1.7		Check that the stored information related to the results of investigations, charging data such as bulk-billing information and CDRs, etc., shall be protected against modifications by man-machine commands.		
	9.1.1.8		Check that Calendar management for operator commands is available and it should be possible to execute any command at any time by attaching a time tag to the command and it should be executed when the system real time matches the time tag.		
	9.1.1.9		Verify that it is possible to store, retrieve a log of commands and responses.		
	9.1.1.10		Verify that it shall not be possible to disturb the logs by man machine command or by any means		
	9.1.2	**System supervision**			
	9.1.2.1		Provision should be there for continuous testing of the system to allow both system quality check and fault indication as and when fault arises.		
	9.1.2.2		Verify that the system provides for print-outs and visual / audible alarms to assist in efficient administration.		
	9.1.2.3		The visual display and the devices for manual control of the different parts of the system should preferably be centralised on a supervisory panel. Details of the displays and the control arrangement should be provided.		
	9.1.2.4		Verify that in case a fault is detected requiring reloading of the program, it is carried out automatically. There should be a provision for manual-loading of the programs / software modules.		
	9.1.3	**Maintenance facilities** :			
	9.1.3.1		Verify that the capability of the system to monitor its own		

			performance and to detect, analyse, locate, and report faults.		
	9.1.3.2		Check that the equipment design should be such that any special care and precautions on the part of the maintenance personnel are kept to an absolute minimum.		
	9.1.3.3		Check that the system supplier has supplied the maintenance spares for a period of 3 years keeping in view MTBF and MTTR. Ensure that at least one spare PCB of each type is supplied.		
	9.1.4	**Diagnostic capabilities**			
	9.1.4.1		Obtain from the supplier details regarding diagnostic programs are normally resident in the on line program. Ensure that the diagnostic capability of the system is such that a minimum human intervention is required and to this end. The procedure for invoking such programs and consulting fault dictionary for diagnostic programs should be obtained from the supplier.		
	9.1.4.2		Check that all the hardware testers necessary for efficient maintenance of the system have been provided. Details of the testers should be indicated.		
	9.1.4.3		Check that the test procedures that are recommended for efficient maintenance of the system have been indicated. This should include details of the tests, their periodicity, etc.		
	9.1.4.4		Ensure that for any malfunction in the system, it initiates a fault message and / or a visual and audible alarm. The fault information should direct personnel to the appropriate maintenance manual for location of the faulty unit for detailed procedures on further action to be taken for rectification of the fault conditions. The classification of alarms in the system should be indicated.		
	Chapter-10 Desirable Requirements				
	10.1.7		Check that the volume of data processed at FMCC should be as per the following criteria :- **Switching System**		

			Input	Volume of data	periodicity	disk storage	
			1) CCS-7 Signalling Links	0.2 Erlangs per link	real time	1 month	
			2)Transaction log/OMC log	1 Mb (average per switch)	6 hrs	2 months	
			3)Databases of analysis routing, charging, subs class of service/ entitlements	5 Mb (average per switch	daily	3 cycles	
			Billing system				
			i)Authorized Subs 2)New subs 3)Subs as per the category such as residential, commercial, govt. service, PCO etc. 4) Class of service 5) OTD lines 6)List of defaulters 7)Disconnection/ reconnection list	(1) to (7) 160K for exchange capacity of 10K lines	daily	6 months	
			8) CDRs of subscribers	1.5 MB per day for	to be collected	2 months	

			an Exge. Initially Of 10K Lines **Commercial System** Advise Notes for service provisioning 10KB for an exge. Of 10K lines Daily 6 months		
	10.1.8.1 **10.1.8.2**		a) Check that each Remote site/ centralized system supports interface to a minimum of two CCS-7 links expandable in steps of 2 links. b) The ultimate capacity of a Remote Site shall be to support interface up to 300 links. c) The ultimate capacity of the Central site shall be to handle 75 remote sites with total no. of signalling links upto 7500.		For centralized site
	10.1.9	**Modularity** :			
	10.1.9.1		Check that two processors work simultaneously either in load sharing basis or hot standby mode. In case of failure of the one of the processor, the other should take full load with zero downtime.		
	10.1.9.2		Check that RAID arrangement is used for secured data storage.		
	10.1.9.3		Check that the configuration meet the processing, storage, input/output, networking requirements including ETHERNET and x.25 adapters.		
	10.1.9.4		Verify that the number of front-end terminals/user work stations are provided as per document.		
	10.1.9.5		Check that there is proper arrangement for the protection against corruption and accidental loss of all the stored data.		
	10.1.9.6		Check that modem, router, mediation devices etc. , for interfacing the FMCC to various systems as per site document have been provided by System Supplier .		
	10.1.9.7		Check that all interface connectors and cables are compatible with equipment in the switching / other systems. No hardware change or		

			augmentation of hardware should be necessary in these systems.		
	10.1.9.8		Check that the system hardware does not pose any problem, due to changes in data and time caused by events such as changeover of millennium / century, leap year etc., in the normal, functioning of the system.		
	10.2	**SOFTWARE REQUIREMENT**			
	10.2.1		Fault Tolerant Software :- Check that the software is capable of providing automatic switch over to the standby subsystems in the event of any software or hardware related problems.		
	10.2.2		The system software shall be open, modular and structured. System Supplier shall develop the software using standard software packages.		
	10.2.3		The software should not pose any problem, due to changes in date and time caused by events such as change over of millennium / century, leap year etc., in the normal functioning of the system.		
	10.2.4		Check that the software rights along with source code have been provided by the system supplier for possible usage of the FMCC at more than one site at the discretion of DOT.		
	10.2.5		Check that the software is written in a High Level Language.		
	10.2.6		Verify that the software conforms to the following characteristics : - i). The system is easy to handle both during installation and day-to-day operations. ii). The functional modularity of the software should permit introduction of changes wherever necessary with least impact on other modules. iii). It should be open-ended to allow addition of new features. iv). Adequate flexibility should be available to easily adopt changes in technological evolution in hardware. V) The design shall be such that propagation of software faults is contained. vi). The software should provide sufficient checks to monitor the		

			correct functioning of the system. vii). Test programs should include fault tracing for detection and localization of system faults. viii). Facilities should be in-built to ensure automatic system reconfiguration on detection of any major software fault.		
	10.3	**Power Supply**	i. The equipment shall be capable of working with an input AC Mains supply of 230 Volts with a tolerance of -15% to 10 % and frequency of 50 Hz ± 2 Hz. Or DC power supply of -48V(varies from - 40V to - 57V). ii. Switching mode Power Supply (SMPS) and VRLA battery to be used shall be as per TEC Generic Requirements No. GR/SMP–01 and GR/BAT-01 Respectively. Power supply and battery shall be modular and expendable to support the ultimate equipment configuration. iii. Check that UPS and other power requirements are as specified by the system supplier.		
	10.4	**Building**			
	10.4.1		Check that buildings shall comply to the following minimum specifications :- Floor Loading 400 Kg/Sq. M. Clear Ceiling Height 2.9 Met.		
	10.4.2		Check that Fluorescent lamps for general lighting to a level of 300 Lux are provided in the switching system buildings.		

GLOSSARY

CDR	Call Detail Record
DAT	Digital Audio Tape
FMCC	Fraud Management and Control Centre
GUI	Graphical User Interface
ILDO	International Long Distance Operators
ILL	Internet Lease Lines
IPLC	Internet Private Lease Circuits
IN	Intelligent Networks
ISD	International Subscriber Trunk Dialing
LAN	Local Area Network
LAP-D	Link Access Protocol for D channel
MSC	Mobile Switching Centre
MTBF	Mean Time Between Failures
MTNL	Mahanagar Telephone Nigam Limited
MTTR	Mean Time To Restore
OTD	Operator Trunk Dial
PABX	Private Automatic Branch Exchange
PCB	Printed Circuit Board
PLMN	Public Land Mobile Networks
PSTN	Public Switched Telephone Network
PVC	Permanent Virtual Connection
QA	Telecom Quality Assurance Circle of BSNL
RAID	Redundant Array of Inexpensive Disks
RAM	Random Access Memory
ROM	Read Only Memory
SCSI	Small Computer System Interface
SDCC	Small Distance Charge Centre
SMPS	Switch Mode Power Supply
STD	Subscriber Trunk Dialing
TEC	Telecom Engineering Centre
UPS	Uninterrupted Power Supply
VC	Virtual Connection
VMC	Voucher Management System
WAN	Wide Area Network

END OF THE DOCUMENT