Government of India
Ministry of Communications
Department of Telecommunications
Telecommunication Engineering Centre
K.L. Bhawan, Janpath, New Delhi-110001
(NGN Division/ एन.जी.एन. प्रभाग)

File No.: 1-1/2025-NGN/TEC/GR-FMCC/3 Date: .06.2025

Subject: Revision of Standard for Generic Requirement (GR) **"FRAUD MANAGEMENT AND CONTROL CENTRE (TEC 58110:2010)"**

In exercise of the powers conferred by rule 5(2) of the Telecommunications (Framework to Notify Standards, Conformity Assessment and Certification) Rules 2025 The draft Standard for Generic Requirement (GR) of **"FRAUD MANAGEMENT AND CONTROL CENTRE (TEC 58110:2010)"** is enclosed herewith for consultation process to enable all stakeholders to provide their comments. The comments may be provided by stakeholders with a soft copy in doc/excel sheet format only, as per the template sheet enclosed herewith as **Annexure-I** through email to director-al.tec-dot@gov.in and ddglte.tec@gov.in at the earliest and latest within sixty days.

Enclosures:

1. Draft Standard No. TEC 58110:2010.
2. Template/Format for providing comments (Annexure-I)

(Rajvinder Singh)
Director(NGN)TEC
Email director-al.tec-dot@gov.in

To,
All Manufacturers and Stakeholders

Copy to:

1. Sr DDG TEC, for kind information
2. AD(IT), TEC – with request for uploading on TEC website/Portal.
3. AD(IMP&TEP) TEC: with a request for uploading on TBT Enquiry Point

Digitally signed by
Rajvinder Singh
Date: 19-06-2025
11:00:01

वर्गीय आवश्यकताओं के लिए मानक

टीईसी 58110:2010

(पूर्वसं:टीईसी/जीआर/एसडब्ल्यू/एफएमसी-01/03 मार्च 10)

STANDARD FOR GENERIC REQUIREMENTS

TEC 58110:2010

(Earlier No: TEC/GR/SW/FMC-01/03 MAR 10)

धोखाधड़ी प्रबंधन और नियंत्रण केंद्र

FRAUD MANAGEMENT AND CONTROL CENTRE

ISO 9001:2015

दूरसंचार अभियांत्रिकी केंद्र
खुर्शीदलाल भवन, जनपथ, नई दिल्ली-110001, भारत
TELECOMMUNICATION ENGINEERING CENTRE
KHURSHIDLAL BHAWAN, JANPATH, NEW DELHI–110001, INDIA
www.tec.gov.in

Release 03: MAR, 2010

Cost: Free of Cost

FOREWORD

Telecommunication Engineering Centre (TEC) is the technical arm of Department of Telecommunications (DOT), Government of India. Its activities include:

- Framing of TEC Standards for Generic Requirements for a Product/Equipment, Standards for Interface Requirements for a Product/Equipment, Standards for Service Requirements & Standard document of TEC for Telecom Products and Services
- Formulation of Essential Requirements (ERs) under Mandatory Testing and Certification of Telecom Equipment (MTCTE)
- Field evaluation of Telecom Products and Systems
- Designation of Conformity Assessment Bodies (CABs)/Testing facilities
- Testing & Certification of Telecom products
- Adoption of Standards
- Support to DoT on technical/technology issues

For the purpose of testing, four Regional Telecom Engineering Centers (RTECs) have been established which are located at New Delhi, Bangalore, Mumbai, and Kolkata.

ABSTRACT

This document specifies the Generic Requirements of Fraud Management and Control Centre (FMCC) for use in the National Network. The FMCC shall be capable of detecting and controlling the frauds in real time as well as near-real time basis.

CONTENTS

Chapter	Title	Page
	History Sheet	2
1.	Introduction	3
2.	System Architecture /Description	7
3.	Functional Requirements of FMCC	10
4.	Interconnectivity and Interoperability Requirements	21
5.	Quality Requirements	22
6.	EMI/EMC Requirements	23
7.	Safety Requirements	26
8.	Security Requirements	27
9.	Other Mandatory Requirements	28
10.	Desirable Requirements	30
	Glossary	34

HISTORY SHEET

S. No.	Title	GR No.	Remarks
1.	Fraud Management and Control Centre	G/FMC-01/01.JUL 99	Issue 01.
2.	Fraud Management and Control Centre	GR/FMC-01/02.MAR 2004	Issue 02.
3.	Fraud Management and Control Centre	(TEC 58110:2010) (Earlier No. TEC/GR/SW/FMC-01/03 MAR 10)	Issue 03. Document number changed as per Revised Numbering scheme of TEC for conversion of existing TEC document to Standard vide document no.4-47/2019-RC/TEC dated 07-09-2020

Note:

1. Since the documents have been renumbered as per revised numbering scheme, kindly refer the Mapping- Listing Table pertaining to old and revised document number available on TEC website www.tec.gov.in/. In case of further clarification, please contact at e mail id adgdoc.tec@gov.in
2. Inside the document, GR may be read as Standard for GR, IR as Standard for IR, SR as Standard for SR and TSTP as TEC Test Guide."

CHAPTER - 1

Introduction

FRAUD SCENARIO IN TELECOM NETWORKS

1.0 General

The frauds in Telecommunication Networks have various forms. They can be broadly classified as

(i) Technical Frauds
(ii) Non-Technical Frauds

1.1 Technical Frauds

Technical fraud is committed either by exploiting the technological deficiencies of the system or by hacking through the in-built securities of the system. Technical Fraud is further classified as,

(i) Technical (External) Frauds
(ii) Technical (Internal) Frauds

1.1.1 Technical (External) Frauds

Technical (External) fraud is committed external to the network by gaining access to the system through hacking. Some of such frauds are given below.

1.1.1.1 Automatic Telephone Line Isolator to penetrate into the secret code/password for dynamic STD lock/ Personal Identification Code (PIN).

1.1.1.2 Accessing the O&M port of the switch from remote and perform opening & closing of telephones or other services. The Password may get leaked through interception or shoulder-surfing or using software applications like keyboard operation loggers, which can collect the complete keyboard operation of a particular session.

1.1.2 Technical (Internal) Frauds

Technical (Internal) fraud is committed by gaining access to the system internally. Some of such frauds are given below.

1.1.2.1 Manipulation of databases of billing, charging, routing, subscribers, etc., and penetrating through the Secret code/password for dynamic STD lock/PIN records etc., using man-machine commands, by authorized/ unauthorized persons, in the switching systems.

1.1.2.2 Changing the equipment number, during preparation of bulk billing tape so that the metering information is transferred to the spare equipment number resulting in non-billing and revenue loss.

1.1.2.3 Withdrawing the detailed billing category and suppressing detailed bill information of a subscriber. In the absence of details of calls, subscriber may dispute the calls as there would not be any proof and the calls could not be established, resulting in billing disputes.

1.1.2.4 Providing STD/ISD facility with/without detailed billing category to STD barred subscribers, resulting in billing complaints.

1.1.2.5 Providing free terminating call category to subscriber, resulting in loss of revenue. This fraud is more so in multi-operator environment.

1.1.2.6 Misuse of certain dangerous commands in the switches causing loss of revenue and also damage the credibility of the service provider.

1.1.2.7 Opening and closing of lines within the billing cycle and avoid billing.

1.1.2.8 **Unauthorized Transiting**: The fraudster makes a long distance call by dialing the STD code of a nearby station followed by the long distance number and the SDCC/local exchange transits the call to the destination. The call is charged as if the call is made to the nearby station. This fraud is possible due to deficiencies of the Transit Exchanges.

1.1.2.9 **Diversion of long distance circuits to unauthorized locations:** E1s from TAX exchanges are diverted to PABX, from where illegal calls are made.

1.1.2.10 **Fraud at billing and commercial centre:** Manipulation of call charge data, subscriber class of service or category etc, at the billing centre or commercial centre.

1.1.2.11 **PABX fraud**: A fraudster by illegal means knows user ID and password to control the administrative commands of the PABX switch and uses them fraudulently. A Large volume of unauthorized national/international calls are made from the PABX switch.

1.1.3 Non-technical Frauds

Some of the non-technical frauds are given below.

1.1.3.1 **Subscription Fraud**: In this type of fraud a subscriber registers for phone service, makes a large phone bill mostly through call selling and runs away before disconnection and becomes a defaulter. Further the subscriber may use a false name and repeat the fraud in the same premises or elsewhere.

1.1.3.2 **Clip-on Fraud**: In this type of fraud, the fraudster accesses the MDF/Pillar/DP and diverts the line and makes calls or sells services to others. The legitimate user denies the usage, resulting in billing complaint.

1.1.3.3 **Data Line Abuse**: The leased data lines which are meant for data transmission are misused for making long distance voice calls by connecting to the circuit to the PSTN at the distant end. At the local end the access to the international network is provided through PSTN dial up lines terminated on a computer based system. This circuit is sometimes sold to others as International Simple Resale. Revenue is lost due to disparity in charging the long distance calls and the leased circuit. The traffic is completely bypassed in some cases and heavy loss occurs to the service provider.

1.1.3.4 **Call Forwarding Fraud**: Call forwarding fraud is performed by forwarding calls to national or international numbers from fraudulently obtained telephone numbers. The fraudster sells the calls and the owner of the number from which calls are forwarded has to pay the bills. This type of fraud could be performed on office telephones during non-working hours. A fraudster may also use his own telephone for selling calls by call forwarding and does not pay the bill. On disconnection he takes a new connection and again repeats the same activity.

1.1.3.5 **Electronic Devices Fraud**: There are devices, which block or interfere with the Answer Signal. Devices are also available which simulate the sound of coins or weight of coins being deposited into a pay phone.

1.1.3.6 **Callback Fraud**: There are various ways of accessing the callback service. One of the ways is a person subscribes to a callback service abroad and

calls a trigger number. The callback system makes a return call to his phone and feeds him the dial tone of the distant country. The person can make international calls on that line at cheaper rates. The FMCC shall be capable of detecting various types of callback services that may come up, time to time.

1.1.3.7 **Three-way calling Fraud**: Using the 3 party conferencing facility, the fraudster sells the calls by putting through large number of long distance calls.

1.1.3.8 **Bypassing of International Traffic** : Grey market operators bypass the authorized network of International Long Distance Operators (ILDO) by establishing unauthorized International link/ connectivity through VSAT Satellite antenna, Internet Lease Lines (ILL), Internet Private Lease Circuits (IPLC), ISDN lines etc. International incoming calls brought through these unauthorized connectivity is then distributed to the National Network PSTN/Mobile connections taken from the local access operators, thus bypassing the licensed networks for carrying the ILD traffic.

1.1.3.9 **IN frauds**

(i)**Premium Rate Service (PRS):** The fraudster sets up PRS with a local service provider or service provider abroad. He or his accomplices makes large number of calls to the PRS and runs away before paying the bill, but collects the revenue from the service providers for the PRS

(ii) **Frauds in 'pre-paid services'** : Frauds related to Pre-paid services are committed at IN platform by manipulation of subscriber databases. Examples of frauds possible in pre-paid services are unauthorized refills or illegal recharging, manipulation of tariff plan, excessive active time (a pre-paid subscriber uses his account even after it expires).

1.1.3.10 **Frauds in Mobile Networks**: The following are some of the mobile frauds.

(i) **SIM card cloning**: Two or more calls from the same subscriber identification number are made at the same time or from geographically separated places with unlikely/unrealistic travel time. This type of fraud is possible by duplicating/cloning the SIM cards.

(ii) **Multiple Call transfer Fraud:** The fraudster sells calls by multiple call transfer using the feature of Mobile handset. The fraudster has no intention to pay the bill. As soon as services expire/barred, a new subscription will be opened using false identity.

(iii) **International Roaming Fraud**: Committing subscription fraud by making Multiple Roaming calls. A subscriber with roaming facility makes large number of international calls and runs away without paying bills.

1.2 SCOPE

1.2.1 This document specifies the Generic Requirements of Fraud Management and Control Centre (FMCC) for use in the National Network.

1.2.2 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.

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

CHAPTER – 2

Description of Network Elements/Component (SYSTEM ARCHITECTURE)

2.0 This chapter gives the architectural over view of an FMCC based on real time as well as near-real time analysis.

2.1 The architecture of the FMCC shall support two configurations as given below.

(i) Centralized Fraud Management and Control Centre
(ii) Standalone Fraud Management and Control Centre

2.1.1 Centralized Fraud Management and Control Centre

A centralized FMCC shall be organized hierarchically with number of remote sites controlled by a single central site. The system architecture shall have typically the following components.

- Remote Site Equipment
- Central Site Equipment
- Wide Area Network (WAN) connecting the Remote Site to the Central Site

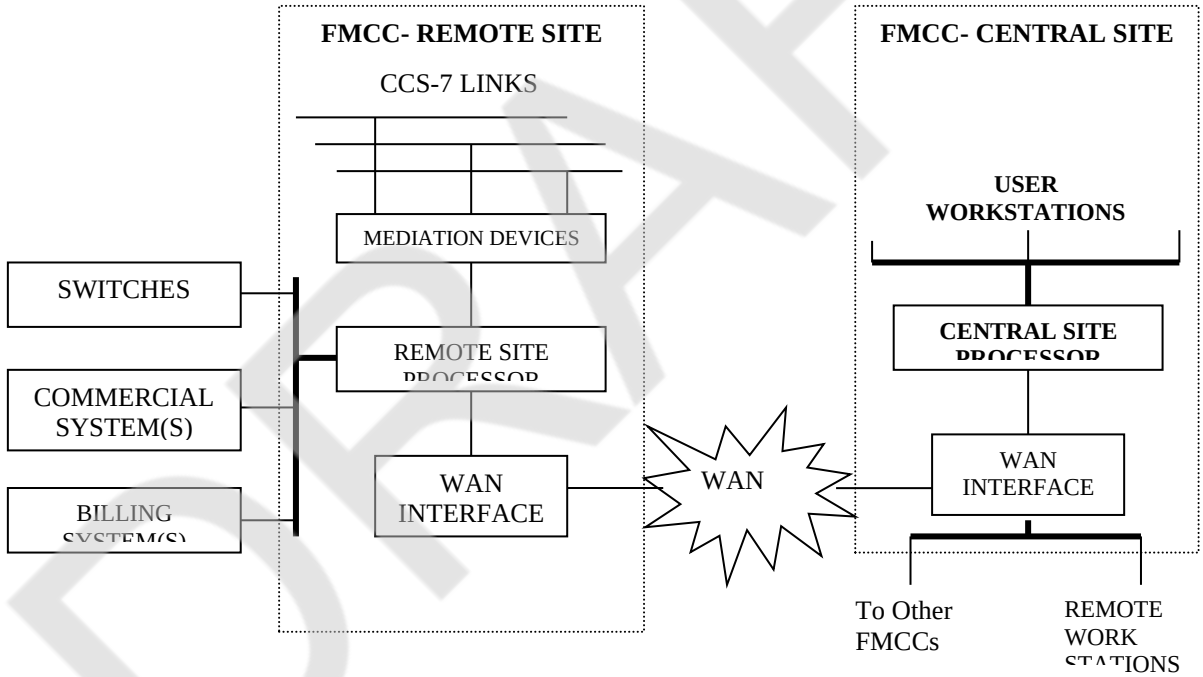


Figure-1: Centralized Fraud Management & Control Centre

2.1.1.1 Remote Site Equipment

The remote site equipment shall be provided at the Transit exchanges. It shall typically contain the following equipment (refer Figure-1).

a) Mediation Device (MD)
b) Remote Site Processor (RSP)
c) Interface to the WAN
d) Interface to switches, billing and commercial systems

2.1.1.1.1 The MD shall retrieve the CCS-7 signaling messages from 2Mbps PCM streams by means of a passive high impedance bridging isolator without

causing any attenuation/loss of signaling information without altering/introducing messages/patterns in the signaling channel.

2.1.1.1.2 The time slot numbers assigned for signaling links on each PCM stream are not fixed and the MD shall be capable of retrieving the information from any time slot automatically / as programmed by the user.

2.1.1.1.3 The RSP shall control a number of mediation devices. It shall collect the data from the mediation devices, filter the desired data, convert into Call Detail Records (CDRs) and transfer the CDRs to the Central Site, through the WAN.

2.1.1.1.4 The RSP shall provide adequate storage capacity to store the CDRs and provide interface devices to backup the system data, CDRs, etc., in a Cartridge 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 The RSP shall be 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 typically contain the following equipment.

a) Central Site Processor (CSP)
b) multi-user Work Stations
c) Interface to the switches, billing and commercial systems
d) Interface to the WAN
e) high speed line printer(s) and
f) Interface to other Central Sites

2.1.1.2.1 The CSP shall be responsible for communicating with the Remote Site and receive the CDR data from the RSP and analyze for detecting various frauds on real time basis.

2.1.1.2.2 The CSP shall be 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.

2.1.1.2.3 The CSP shall provide adequate number of user workstations based on GUI interface for interacting with the system. The workstations and the CSP shall be connected in a LAN and it shall be possible to connect remotely located PC/terminals for operating the system from remote.

2.1.1.2.4 The CSP shall support operation and maintenance of the entire system including the Remote Site Equipment and the WAN.

2.1.1.2.5 The CSP shall optionally provide necessary interface for transmitting desired data to another Central Site. The interface shall be on X.25/X.28 protocol on 2w/ 4w leased circuits.

2.1.1.2.6 The CSP shall provide adequate storage capacity to store the CDRs and provide I/O devices to backup the system data, CDRs, etc. in a Cartridge Tape/DAT.

2.1.2 Standalone Fraud Management and Control Centre

2.1.2.1 A standalone fraud management & control centre shall be an independent centre with the entire equipment located at one site.

2.1.2.2 A standalone system is deployed in such segments of the network where there is only one Transit Exchange or all the CCS-7 links required to be monitored are available at one point and there are limited number of links and systems to be interfaced.

2.1.2.3 The standalone system shall have all the functionalities of a centralized system.

2.1.2.4 The system architecture shall have typically the following components (Fig-2).

a) Mediation Device (MD)
b) Site Processor (SP)
c) Multi-user Work Stations
d) Interface to the switches, billing and commercial systems
e) High speed line printer and
f) Interface to Central Sites

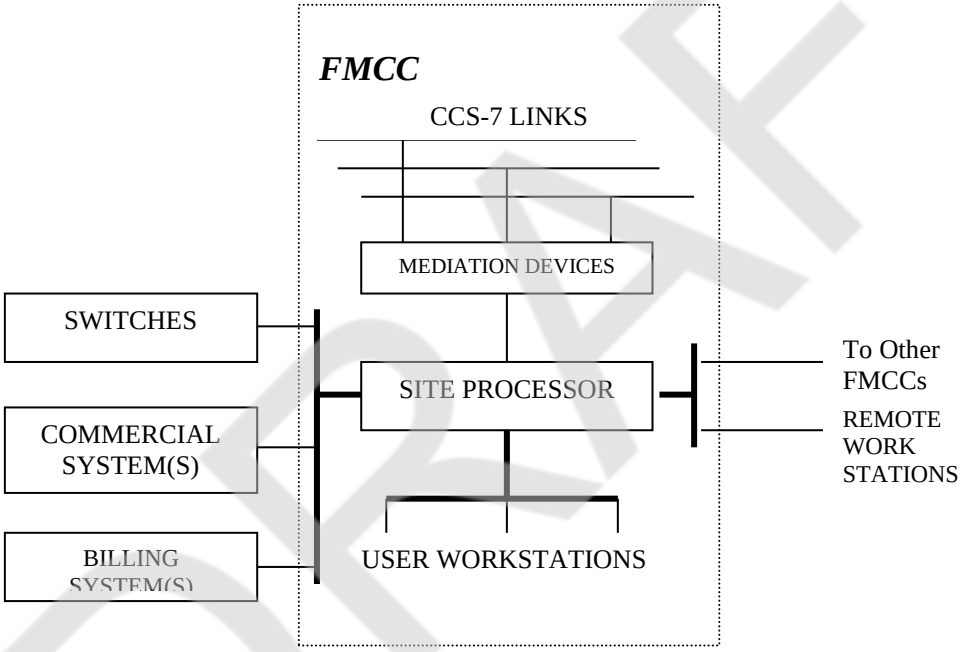


Figure-2: Standalone Fraud Management & Control Centre

CHAPTER – 3

Functional Requirements

3.0 Introduction

This chapter contains the functional requirements of the FMCC for method of detection, the inputs for analysis, detection techniques, detection and analysis and fraud control and counter measures.

3.1 General Requirements

The FMCC shall derive the inputs for analysis from various sources through appropriate interfaces and connections. This chapter gives the interface requirements with various systems.

3.1.1 The supplier shall provide necessary hardware and software, and mediation devices, line interfacing equipment, etc., required to interconnect the FMCC to various systems for collecting the inputs.

3.1.2 The supplier shall carryout necessary modifications in the software and hardware if required to inter-work with these systems.

3.1.3 The FMCC shall be capable of accepting and analyzing the inputs in different formats depending on the system to which it is interfaced.

3.1.4 **Switching Systems**

a) The FMCC shall build the Call Detail Records (CDRs) from the CCS-7 signalling links on the routes viz., Inter-TAX, TAX-International Gateway exchanges, TAX to TAXs of neighboring countries, Mobile Switching Centre (MSC), Signalling Transfer Points (STP) and Point of Interconnect with PLMN and PSTN operators. (refer Figure-1).

b) Transaction log/OMC log

c) Databases of analysis, routing, charging, subscriber Class of Service/entitlements

3.1.5 **Billing System**

The FMCC shall retrieve the following information from billing system, based on which the detection shall be done.

(i) Authorised subscribers list with name, address, account number, network type (fixed or mobile) and all relevant details from the billing system.
(ii) New Subscribers list with name, address, account number, network type (fixed or mobile) and all relevant details from the billing system.
(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/black listed subscribers.
(vii) Disconnection/reconnection lists.
(viii) CDRs of subscribers.
(ix) Fortnightly Call charge readings.

3.1.6 **Commercial System**

The FMCC shall retrieve the database of Advise Notes for service provisioning from the commercial system(s).

3.1.7 **Leased Data Circuits**

The system shall be capable of extracting the signalling interchanged on the Leased Data Circuits for detecting **Data line abuse Fraud** as explained in the Clause No. 1.1.3.3. The Data Circuits are required to be normally interfaced at the Transmission Stations.

3.1.8 The supplier shall specify any other information required for analysis along with the interface requirements.

3.2 **Detection of Fraud**

3.2.1 The FMCC shall detect various frauds discussed in Chapter-2 in **Real Time** as well as **Near Real Time** as given in the table below and apply control or provide support in decision making by recommending counter actions.

A. Real time detection

Nature of fraud	Reference Clause No.	Method of detection
Technical (External) Automatic Telephone Line Isolator	**1.1.1.1**	Call Thresholds and profile deviation check.
Technical (Internal)		
(i) Providing STD/ISD facility with/without detailed billing category to STD barred subscribers	**1.1.2.4**	From CDR generated by FMCC and subscriber profile / subscriber database.
(ii) Providing free terminating call category to subscriber	**1.1.2.5**	From CDR generated by FMCC.
(iii) Diversion of long distance circuits to unauthorized locations	**1.1.2.9**	From CDR generated by FMCC (No CLI or CLI not mapped in FMCC).
(iv) PABX fraud	**1.1.2.11**	From CDR generated by FMCC, threshold and profile deviation check.
Non-technical Frauds		
(i) Clip-on Fraud	**1.1.3.2**	Call thresholds and profile deviation check.
(ii) Call forwarding/Multiple call forwarding fraud	**1.1.3.4**	Threshold and profile deviation check.
(iii) Electronic Devices Fraud	**1.1.3.5**	From CDR generated by FMCC.
(iv) Call back fraud	**1.1.3.6**	From CDRs generated by FMCC, threshold, destination check and profile deviation check.
(v) Three way calling	**1.1.3.7**	From CDRs generated by FMCC, threshold and profile deviation check.
(vi) Bypassing of International	**1.1.3.8**	From CDRs generated by FMCC, threshold, destination check and

traffic		profile deviation check.
(vii) Premium Rate Service	**1.1.3.9(i)**	Threshold and profile deviation check. Geographical / velocity check.
(viii) Mobile Frauds	**1.1.3.10**	Threshold, destination and profile deviation check.

B. Near Real time detection

Nature of fraud	Reference Clause No.	Method of detection
Technical (External) (i) Accessing the O&M port of the switch from remote and perform opening & closing of telephones or other services	**1.1.1.2**	By analysis of switch Log and Advice Note from commercial centre. or By processing the data from billing centre / commercial centre and the data generated by FMCC from CDRs.
Technical (Internal) (i) Manipulation of databases of billing, charging, routing, subscribers	**1.1.2.1**	Switch log and comparing OMC files with the previous day.
(ii) Changing the equipment number, during preparation of bulk billing tape	**1.1.2.2**	By analysis of Switch Log and Advice Note.
(iii) Withdrawing the detailed billing category and suppressing detailed bill information of a subscriber	**1.1.2.3**	By analysis of Switch Log and Advice Note.
(iv) Misuse of certain dangerous commands in the switches	**1.1.2.6**	By analysis of Switch Log and Advice Note.
(v) Unauthorized Transiting at TAX	**1.1.2.8**	By analysis of System routing and charging files.
(vi) Fraud at billing and commercial centre.	**1.1.2.10**	By processing the data from billing centre / commercial centre and the data generated by FMCC from CDRs.
(vii) Pre-paid fraud	**1.1.3.9(ii)**	By Analyzing data from Voucher Management System (VMC) and data base generated by FMCC from CDRs.
Non-technical Frauds (i) Data Line Abuse	**1.1.3.3**	FMCC shall detect normally used protocols for voice on data line by itself or through Protocol Analyzer.

3.3 Real Time Detection

3.3.1 The Real Time detection shall be based on the analysis of messages on the CCS-7 signaling links.

3.3.2 The FMCC shall provide necessary mediation device/probe to extract the CCS-7 signaling messages.

3.3.3 **Inputs for Analysis**

3.3.3.1 The FMCC shall build 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, Mobile Switching Centre(MSC), Signaling Transfer Points (STP) and Point of Interconnect with PLMN and PSTN operators (refer Figure-3).

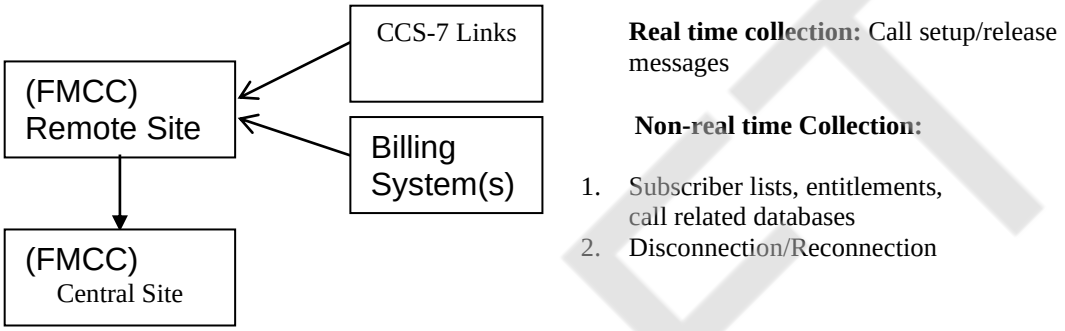


Figure 3: Inputs for Real Time Analysis

3.3.3.2 The FMCC shall retrieve the following information from billing system, based on which the real time detection shall be done.

(i) Authorized subscribers list with name, address, account number, network type (fixed or mobile) and all other relevant details.

(ii) New Subscribers list with name, address, account number, network type (fixed or mobile) and all other 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/black listed subscribers.

(vii) Disconnection/reconnection lists

(viii) CDRs of subscribers

(ix) Fortnightly Call charge readings

3.3.4 **Detection Techniques**

3.3.4.1 The fraud detection shall be based on the analysis of certain key parameters to detect probable causes of frauds.

3.3.4.2 The basic parameters for detection shall be user- definable and are based on business and subscriber related policies of service provider.

3.3.4.3 The FMCC shall use these parameters for prioritizing the fraud.

3.3.4.4 It shall be possible to change the rules, create new rules or combine rules to detect new scenarios time to time as per the requirement, by the user.

3.3.4.5 The detection shall be through various techniques. Some of the techniques are given below.

(i) **Threshold:** The FMCC shall detect crossing of threshold, for the duration of call, value of call, number of calls, total usage and cost, etc. The threshold shall be user programmable and can be set for group(s) of subscribers.

(ii) **Call Patterns:** The FMCC shall compare the contents of any field(s) in the CDR with the pre-defined data and generate alerts whenever the call parameters match the defined rule conditions. The pattern shall be created by the user/system and updated automatically by the system. The pattern may be calling number, called number, access code of a station, etc.

(iii) **Geography/Velocity Check:** Detection of calls from geographically separated places with unlikely/unrealistic travel times, originated with a single telephone identification number.

(iv) **Profile Comparison:** The information about the subscriber's normal calling behavior is called profile. Profiles are based upon a period of observed behavior and contains calling frequency, duration, charges etc. The FMCC shall generate alerts whenever serious deviations from normal behavior values are detected by comparing with the profile.

(v) **Destination Check:** Detection by checking whether the called number is figuring in the normally called destinations by individual subscribers.

3.3.5 **Detection and Analysis**

3.3.5.1 The FMCC shall effectively detect frauds based on advanced mathematical statistical algorithms, correlation using mathematical models, etc. A detailed explanation with flow charts for the logic of detection and analysis of frauds in real time shall be provided by the supplier.

3.3.5.2 The FMCC shall use the information collected initially from the billing centre and commercial centre, for generating the subscriber profiles of each subscriber to show specific calling behavior and destinations called, for both working days and holidays.

3.3.5.3 Subsequently, the FMCC shall update subscriber profiles from the CDRs generated from the CCS-7 messages.

3.3.5.4 The subscriber profiles shall be updated by the FMCC based on usage days defined by System Administrator (normally 10 to 30 days). The system shall be able to display the details of subscriber(s) profile using MMC.

3.3.5.5 The subscriber profile (in accordance with clause 3.3.5.2 and 3.3.5.3) shall contain typically the 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 STD/ISD call made during different time bands.

(iv) Average duration per STD/ISD call made during different time bands.

(v) Average number of STD/ISD Calls made during different time bands.

(vi) Accumulated charges of STD/ISD calls made during normal-day/peak-day/ Sunday/ holiday week/month.

(vii) Average number of STD/ISD calls made during normal-day/peak-day/Sunday/ holiday/week/month.

(viii) Number of long duration calls made during different time bands.

(ix) Number of long duration calls made during normal-day/peak-day/Sunday/ holiday/week/month.

(x) Average charge per premium rate call during different time bands.

(xi) Average duration per premium rate call made during different time bands.

(xii) Average number of premium rate calls during different time bands.

(xiii) Accumulated charges of premium rate calls made during normal-day/peak-day/Sunday/holiday week/month.

(xiv) Number of premium rate calls made during normal-day/peak-day/Sunday/ holiday/week/month

(xv) Frequently called national/international destinations.

(xvi) Number of incoming STD/ISD calls per normal-day/peak-day/Sunday/holiday/ week/month.

(xvii) Number of calls forwarded during different time bands.

(xviii) Number of calls forwarded during normal-day/peak-day/Sunday/holiday/ week/month.

It shall be possible to add a new field or delete a field by the System Administrator in the subscriber profile.

3.3.5.6 The FMCC shall support applying above thresholds for various time bands as per the tariff structure for national and international calls (varies for groups of countries), which may change from time to time as per the policies of service provider.

3.3.5.7 The CDRs generated by FMCC shall be compared with the data of subscriber profile to generate profile deviation alarms.

3.3.5.8 **Check List/ Hot List/ Black List:** A Check List/ Hot List/ Black List is a list containing calling subscriber numbers, called number, destination codes or any other data with which the corresponding fields of each CDR generated by FMCC shall be checked in real time to generate alerts. 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

3.3.5.9 The FMCC shall support minimum twenty Check List/ Hot List/ Black List, which are user programmable. The FMCC shall provide necessary tools to create/ modify/ delete the list by the System Administrator.

3.3.5.10 **Exception List :** An Exception List is a list containing certain fields to prevent generation of alarms for certain entries in the lists. The entries in the exception lists shall be user programmable.

3.3.5.11 The CDRs generated by the FMCC shall be checked against the entries in the Check List/ Hot List/ Black List and exceptional list(s) to generate alerts.

3.3.5.12 **Threshold List :** A Threshold List contains the usage parameters of calls, based on which threshold alarms are generated. The FMCC shall support sets of Threshold Lists, which shall be defined based on the group(s) of subscribers. The thresholds shall be typically,

a) Charge per STD/ISD Call for each time band.
b) Duration per STD/ISD Call for each time band.
c) Number of STD/ISD Calls for each time band.
d) Number of STD/ISD Calls during normal day/peak day/Sunday/ holiday/week/ month.
e) Accumulated charges of STD/ISD Calls per normal-day/peak-day/ Sunday/holiday/ 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 for each time band and per normal-day/peak-day/Sunday/holiday/week/month.
h) Charge, duration and number of calls forwarded to STD/ISD for each time band and per normal-day/peak-day/Sunday/holiday/week/month.

The FMCC shall generate alerts, if any of the above threshold limit is crossed.

3.3.5.13 The FMCC shall provide a tool to define different ‘rules’ to set ‘Call Patterns’ (refer 3.3.4.5 (ii)) by the user.

(i) It shall be possible to combine ‘Call Patterns Rule’ logically.
(ii) It shall be possible to define a new rule on any field of the CDR.
(iii) It shall be possible to modify/delete an existing rule.
(iv) It shall be possible to display/print all defined rules.

3.3.5.14 The FMCC shall be able to automatically define new rules to be applied, based on pattern of calls, calling trends, correlation using mathematical model, etc, to detect frauds.

3.3.5.15 The FMCC shall perform Geography /Velocity checks in case of Mobile calls.

3.3.5.16 The FMCC shall support prioritization of the alerts into frauds based on the following weighting factors.

(i) Type of threshold and the number 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 The system shall have an advanced analysis capability to correlate the frauds under investigation with the previously identified frauds and use relevant data for detection of frauds.

3.3.5.18 FMCC shall generate the alarm for real time fraud detection within 5 minutes from the arrival of condition.

3.3.5.19 The FMCC shall generate the prioritized cases as above giving the following details and store them for further investigation.

a. Case number,
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

3.4.1 The Near Real Time detection shall be based on the analysis of relevant databases from switching systems & commercial/billing systems.

3.4.2 The FMCC shall provide necessary mediation devices to extract the databases from switching systems & commercial/billing systems.

3.4.3 Inputs for Analysis

3.4.3.1 The FMCC shall retrieve 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

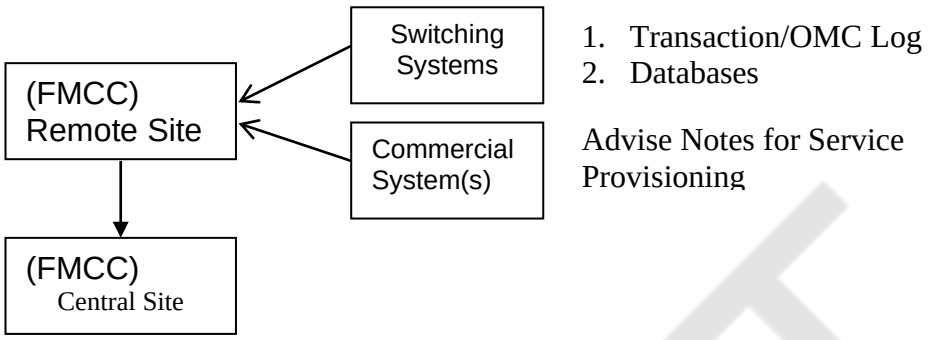


Figure 2: Inputs for Near Real Time Analysis

3.4.4 **Detection Methodology**

3.4.4.1 The FMCC shall perform data integrity & audition as follows.

(i) The Transaction/OMC log,

(a) Shall be checked for certain dangerous commands,

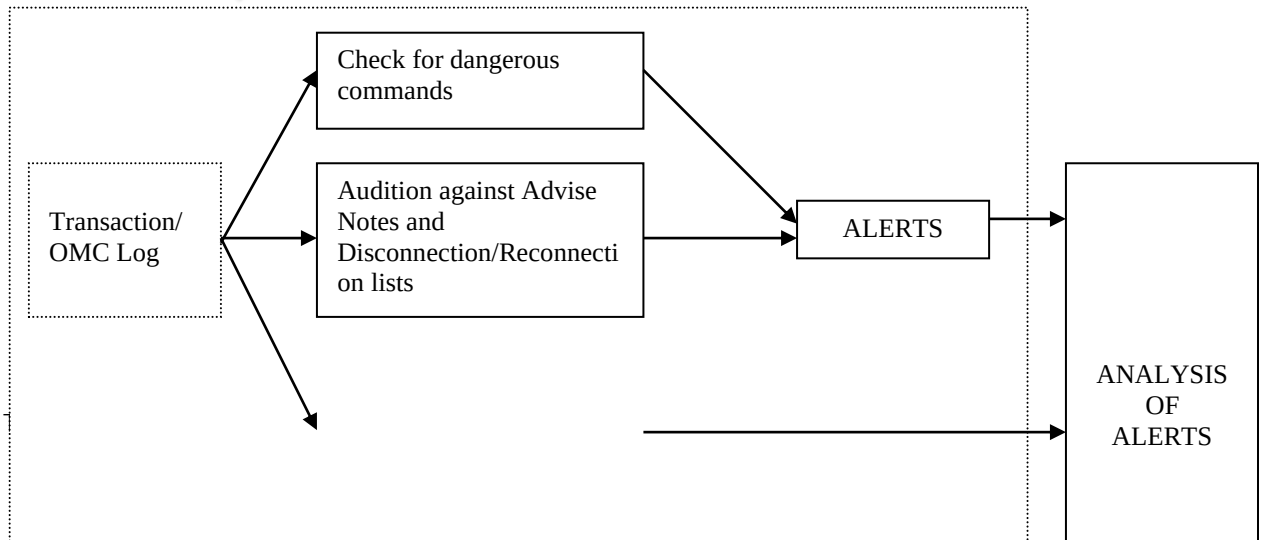
(b) The subscriber management commands shall be audited against a valid Advise Note or disconnection/reconnection order

(ii) (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 The FMCC shall 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 The FMCC shall generate listings of analysis, routing and subscribers from the above databases and store in the central site.

3.4.4.4 The FMCC shall be capable of accepting the inputs in different formats that may vary from system to system.



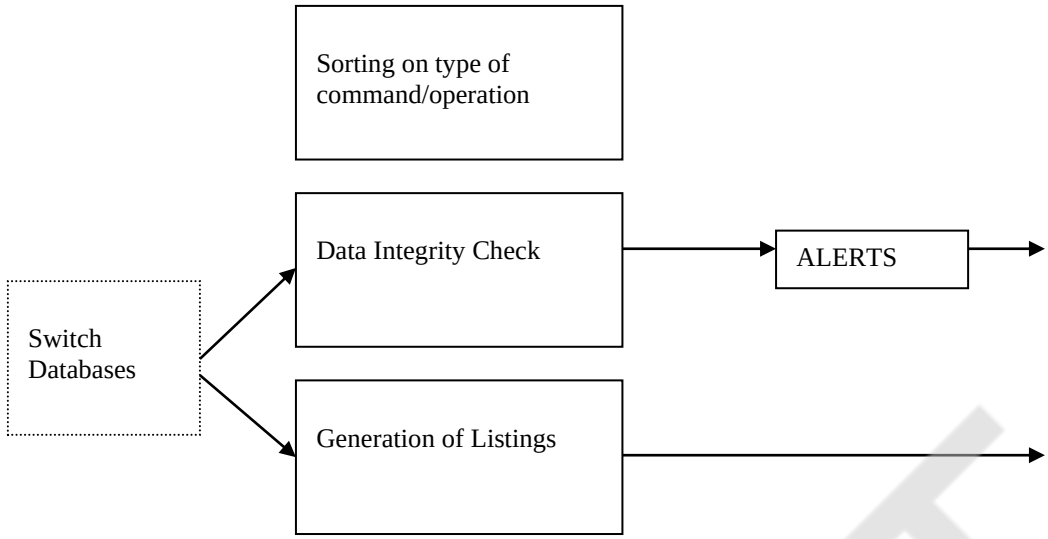


Figure 3: Near Real Time Detection and Analysis

3.4.4.5 **Fraud at billing and commercial centre**

The FMCC shall check the data integrity of the billing information received from billing centre against the 'Advise Note' (issued for service provisioning) data, received from Commercial centre. Any disparity in the billing amount shall also be checked from the database generated from the CDRs. In case of any mismatch an alert shall be generated.

3.5 **Fraud Control & Counter Measures**

3.5.1 The FMCC shall support automatic control of the fraud as given below.

(i) The system shall support 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 shall be different for each type of switching system.

(ii) The system shall indicate 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, the system shall initiate 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) The system shall capture the responses of the switching system based on which it shall indicate the results.

3.5.2 The system shall also support execution on the high level commands/macros for the above operations, on demand by the fraud investigator as per 3.4.1(iii) & (iv).

3.5.3 The automatic and on demand operation shall be provided through password access.

3.6 The FMCC shall give an audio and visual alarm or send SMS / e-mails on detecting high priority fraud (user definable), so that an immediate action can be taken.

3.7 FMCC shall update the STD/ISD/ MSC/Local Switch Code list from the CDRs generated by it.

3.8 FMCC shall update the Premium rate service numbers list from the CDRs generated by it.

3.9 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 FMCC shall provide an easy method to update the system database, for bulk data changes like change in local area code or bulk transfer of numbers.

3.11 The FMCCs of different zones shall be inter-linked for query/exchange of data for investigations.

3.12 The FMCC shall monitor 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 The FMCC shall monitor the traffic/load on each CCS-7 link and update at least once in 3 minutes and report.

3.14 FMCC shall generate a report on how many CDRs generated, how many of them processed and how many of them dropped for various reasons.

CHAPTER – 4

Interconnectivity and Interoperability Requirements

4.1 Interface with Switching Systems

4.1.1 **Interface for Signalling Links :** For the input mentioned at para 3.1.4 (a): The National standards for the CCS-7 signalling are specified in the TEC standard No.S/CCS-02 and in TEC Generic Requirements No. G/TAX-01 for International Gateway function of TAXs, shall be applicable.

4.1.2 **Interface for retrieving office-data :** For the input mentioned at para 3.1.4 (b)&(c): X.25 protocol using X.21 bis-V.24 (baud rate of 9600) as the physical layer for collecting inputs and issuing commands shall be applicable.

4.1.2.1 In addition the FMCC shall also support physical layer on X.21 (baud rate of 64 kbps).

4.1.2.2 LAPB shall be supported for layer 2.

4.1.2.3 The FMCC shall support dialogue with switch on Virtual Call (VC) as well as Permanent Virtual Circuit (PVC) for layer 3.

4.1.2.4 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.

4.1.2.5 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

4.2.1 The FMCC shall be capable of interfacing with the Billing and Commercial Systems of Service Provider in a LAN/WAN configuration.

4.2.2 The FMCC shall interact with various systems in the language which is specific to each system without calling for any changes in the existing systems

4.3 Wide Area Network (WAN)

The WAN shall provide the communication between the RSPs and CSP. 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 It shall also be possible to manually copy the inputs (other than CCS-7 messages) from storage medium such as floppy, Magnetic Tape, Cartridge Tape, DAT tape, optical disk etc.

Chapter -5

Quality Requirements

5.1 Qualitative Requirements (QR)

5.1.1 The supplier/manufacturer shall conform to ISO 9001:2008 certifications. A quality plan describing the quality assurance system followed by the manufacturer shall be required to be submitted. Alternatively the equipment shall be manufactured as per guidelines issued by Quality Assurance wing (QA) of purchaser.

5.1.2 The failure of any component/subsystem in the system shall not result in the failure of complete system.

5.1.3 List of all components for which second source is not available should be provided.

5.2 Reliability

5.2.1 The FMCC shall be able to work in full redundant configuration and shall support disaster recovery .

5.2.2 FMCC shall support 1+1 redundancy with all the critical components having N+1 redundancy.

Chapter -6

EMI/EMC Requirements

6.1 Electromagnetic Interference : The equipment shall conform to the following EMC requirements for Class A:

I. General Electromagnetic Compatibility (EMC) Requirements: - The equipment shall conform to the EMC requirements as per the following standards and limits indicated therein. A test certificate and test report shall be furnished from a test agency.

a) Conducted and radiated emission *(applicable to telecom equipment)*:
Name of EMC Standard: "CISPR 22 (2005) with amendment 1 (2005) & amendment 2 (2006) - Limits and methods of measurement of radio disturbance characteristics of Information Technology Equipment".

Limits:-
i) To comply with Class A (to be mentioned in the GR / IR as per the specific requirement) of CISPR 22 (2005) with amendment 1 (2005) & amendment 2 (2006).

ii) The values of limits shall be as per TEC Standard No. TEC/EMI/TEL-001/01/FEB-09**.**

b) Immunity to Electrostatic discharge:
Name of EMC Standard: IEC 61000-4-2 {2001) "Testing and measurement techniques of Electrostatic discharge immunity test".

Limits: -
i) Contact discharge level 2 {± 4 kV} or higher voltage;

ii) Air discharge level 3 {± 8 kV} or higher voltage;

c) Immunity to radiated RF:
Name of EMC Standard: IEC 61000-4-3 (2006) "Testing and measurement techniques-Radiated RF Electromagnetic Field Immunity test"

Limits:-
For Telecom Equipment and Telecom Terminal Equipment with Voice interface (s)
i) Under Test level 2 {Test field strength of 3 V/m} for general purposes in frequency range 80 MHz to 1000 MHz and

ii) Under test level 3 (10 V/m) for protection against digital radio telephones and other RF devices in frequency ranges 800 MHz to 960 MHz and 1.4 GHz to 6.0 GHz.

For Telecom Terminal Equipment without Voice interface (s)
Under Test level 2 {Test field strength of 3 V/m} for general purposes in frequency range 80 MHz to 1000 MHz and for protection against digital radio

telephones and other RF devices in frequency ranges 800 MHz to 960 MHz and 1.4 GHz to 6.0 GHz.

d) Immunity to fast transients (burst):

Name of EMC Standard: IEC 61000- 4- 4 {2004) "Testing and measurement techniques of electrical fast transients/burst immunity test"

Limits:-

Test Level 2 i.e. a) 1 kV for AC/DC power lines; b) 0. 5 kV for signal / control / data / telecom lines;

e) Immunity to surges:

Name of EMC Standard: IEC 61000-4-5 (2005) "Testing & Measurement techniques for Surge immunity test"

Limits:-

i) For mains power input ports : (a)1.0 kV peak open circuit voltage for line to ground coupling (b) 0.5 kV peak open circuit voltage for line to line coupling

ii) For telecom ports : (a) 0.5 kV peak open circuit voltage for line to ground (b) 0.5 KV peak open circuit voltage for line to line coupling.

f) Immunity to conducted disturbance induced by Radio frequency fields:

Name of EMC Standard: IEC 61000-4-6 (2003) with amendment 1 (2004) & amd. 2 (2006) "Testing & measurement techniques-Immunity to conducted disturbances induced by radio- frequency fields "

Limits:-

Under the test level 2 {3 V r.m.s.}in the frequency range 150 kHz-80 MHz for AC / DC lines and Signal /Control/telecom lines.

g) Immunity to voltage dips & short interruptions (applicable to only ac mains power input ports, if any):

Name of EMC Standard: IEC 61000-4-11 (2004) "Testing & measurement techniques- voltage dips, short interruptions and voltage variations immunity tests"

Limits:-

i) a voltage dip corresponding to a reduction of the supply voltage of 30% for 500ms(i.e. 70 % supply voltage for 500 ms)

ii) a voltage dip corresponding to a reduction of the supply voltage of 60% for 200ms; (i.e. 40% supply voltage for 200ms) and

iii) a voltage interruption corresponding to a reduction of supply voltage of > 95% for 5s.

Note 1: The test agency for EMC tests shall be an accredited agency and details of accreditation shall be submitted.

Alternatively EMC test report from a non-accredited test lab, which is audited by an accredited lab / accrediting authority for the availability of all the essential

facilities (test equipment, test chamber, calibrations in order, test instructions, skilled personnel etc.), required for performing the tests according to the EMC test methods audited, may be acceptable.

However, such accredited lab / accrediting authority should take responsibility of the test results of the "non accredited lab" along with indication of period of such delegation and the submitted test report should be of such valid period of delegation. The audit report, mentioning above facts, should be provided along with EMC test report.

Note 2 :- For checking compliance with the above EMC requirements, the method of measurements shall be in accordance with TEC Standard No. TEC/EMI/TEL-001/01/FEB-09 and the references mentioned therein unless otherwise specified specifically. Alternatively, corresponding relevant Euro Norms of the above IEC/CISPR standards are also acceptable subject to the condition that frequency range and test level are met as per above mentioned sub clauses (a) to (g) and TEC Standard No. TEC/EMI/TEL-001/01/FEB-09. The details of IEC/CISPR and their corresponding Euro Norms are as follows:

IEC/CISPR	**Euro Norm**
CISPR 11	EN 55011
CISPR 22	EN 55022
IEC 61000-4-2	EN 61000-4-2
IEC 61000-4-3	EN 61000-4-3
IEC 61000-4-4	EN 61000-4-4
IEC 61000-4-5	EN 61000-4-5
IEC 61000-4-6	EN 61000-4-6
IEC 61000-4-11	EN 61000-4-11

Chapter -7

Safety Requirements

7.1 Safety Requirements

7.1.1 The operating personnel should be protected against shock hazards as per IS 8437 {1993} “Guide on the effects of current passing through the human body” [equivalent to IEC publication 60479-1{1984}].

7.1.2 The equipment shall conform to IS 13252 {2003} “Safety of information technology equipment including electrical business equipment” [equivalent to IEC publication 60950 {2001}] and IS 10437 {1986} “Safety requirements of radio transmitting equipments” [equivalent to IEC publication 60215].

Chapter -8

SECURITY REQURNMENTS

8.1 Security aspects

(i) The Network and the FMCC shall be protected against intentional and accidental abuse, unauthorized access and loss of communication.

(ii) The FMCC security features shall include operator authentication, command, menu restriction and operator privileges. The FMCC shall support four level of password.

(iii) FMCC shall allow the system administrator to define the level of access to the network cap[abilities or features for each assigned password. The FMCC shall block the access to the operator in case of unauthorized command being tried for five consecutive times. The FMCC shall not allow entry to FMCC in case wrong password is provided more than three consecutive times during the login.

(iv) The system supervisor shall be able to monitor and log all operator activities in the FMCC.

(v) The dynamic password facility shall be provided in which the operator change his password at any time.

(vi) The system supervisor shall have the facility of restricting the use of certain commands or procedures to certain password and terminals.

(vii) Secure network arrangements shall be provided between FMCC and the switches, billing systems, commercial systems etc. to ensure that required data should not reaches to any unauthorized person.

(viii) System shall be secured against computer based viruses.

CHAPTER -9

OTHER MANDATORY REQUIREMENTS

9.1 SYSTEM OPERATION AND MANAGEMENT

The system shall be so designed as to enable economic and flexible handling of system administration, maintenance supervision and performance measurements.

9.1.1 System administration

9.1.1.1 A user-friendly GUI (Graphical-User-Interface) based on WINDOWS or any other environment shall be provided for easy administration of FMCC. It shall support the management of databases, initialization, interrogation, modification and deletion of various user programmable parameters and global parameters.

9.1.1.2 Man-machine language shall be in English by providing English based commands and responses.

9.1.1.3 It shall also be possible to carry out operations by issuing commands from a remote centre.

9.1.1.4 Suitable safeguards shall be provided in the man-machine communication programs to debar unauthorized persons from accessing the databases.

9.1.1.5 Access to system operations shall be controlled through multi-level password and authentication checks.

9.1.1.6 The man-machine language shall have facility for restricting the use of certain commands or procedures to certain staff/terminals.

9.1.1.7 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, or any other means.

9.1.1.8 Calendar management for operator commands shall be available. (It shall be possible to execute any command at any time by attaching a time tag to the command and it shall be executed when the system real time matches the time tag).

9.1.1.9 It shall be possible to store, retrieve a log of commands and responses.

9.1.1.10 It shall not be possible to disturb the logs. All system logs shall be protected against modification by man-machine commands or by any other means.

9.1.2 System Supervision

9.1.2.1 Provision shall be made for continuous testing of the system to allow both system quality check and fault indication as a fault arises.

9.1.2.2 The system shall provide for printouts 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 shall preferably be centralized on a supervisory panel. Details of the displays and the control arrangement shall be provided.

9.1.2.4 In case a fault is detected requiring reloading of the program, this shall be carried out automatically. There shall be a provision for manual loading of the programs/software modules.

9.1.3 Maintenance facilities

9.1.3.1 The system shall have the capability to monitor its own performance and to detect, analyze, locate, and report faults.

9.1.3.2 The equipment design shall 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 The maintenance spares supplied shall take into account the MTBF and MTTR The supplier shall accordingly supply number of spares for a period of 3 years. At least one spare PCB of each type shall be supplied.

9.1.4 Diagnostic capabilities

9.1.4.1 The diagnostic capability of the system shall be such as to minimize the human efforts required. To this end, the supplier shall indicate how much of the diagnostic programs are normally resident in the on line program. Details of the off-line diagnostic programs shall be given. The procedure for invoking such programs shall be described. The procedure for consulting fault dictionary for diagnostic programs shall be made available.

9.1.4.2 All the hardware testers necessary for efficient maintenance of the system shall be provided. Details of the testers shall be indicated.

9.1.4.3 The test procedures that are recommended for efficient maintenance of the system shall be indicated. This shall include details of the tests, their periodicity, etc.

9.1.4.4 Any malfunction in the system shall initiate a fault message and/or a visible and audible alarm. The fault information shall direct personnel to the appropriate maintenance manual for location of the faulty unit or for detailed procedures on further action to be taken for rectification of the fault conditions. The classification of alarms in the system may be indicated.

Chapter-10

Desirable Requirements

This chapter covers the Generic Requirements for procurement purposes. Purchaser shall have to specify the requirements in respect of different clauses including, but not limited to the following

10.1 HARDWARE REQUIREMENTS

This covers the hardware requirements of the Remote Site and Central Site equipment of the Centralized Fraud Management and Control Centre as well as Standalone Fraud Management and Control Centre.

10.1.1 The hardware requirements of a remote site equipment of centralized FMCC vary from site to site depending upon the number of signaling links to be monitored.

10.1.2 The hardware requirements of the central site equipment depend on the number of remote sites it serves, signaling links and the extent of near-real time analysis required to be done.

10.1.3 The hardware requirements of the standalone system depend on the number of signaling links and the extent of near real time analysis required to be done.

10.1.4 The Supplier shall provide details of the hardware platform including the details for dimensioning of Hardware Equipment. The hardware shall be state-of-the art, proven, modular and expandable.

10.1.5 The FMCC shall be scalable to allow for adding new features, applications and system integration. The system components shall be scalable and modular to support addition of applications for new requirements.

10.1.6 The following requirement is applicable for both Centralized and standalone FMCC.

10.1.7 **Volume of Data**

Input	Volume of data	Periodicity	Disk Storage
Switching Systems			
a) CCS-7 signalling links	0.2 Erlangs per link.	Real time	1 Month
b) Transaction log/OMC log	1 Mb (average per switch)	6 hrs	2 Months
c) Databases of analysis, routing, charging, subscriber Class of Service/ entitlements	5 Mb (average per switch)	daily	3 cycles
Billing System			
(i) Authorized subscribers (ii) New Subscribers (iii) Subscribers as per the category such as residential,	(i) to (vii): 160 K (for the exchange capacity of 10K lines)	Daily	6 months

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	(viii): 1.5 MB per day for Exchange Capacity of 10K lines	To be collected initially	2 months
Commercial System Advise Notes for service provisioning	10KB for an Exchange Capacity of 10K lines	Daily	6 months

10.1.8 **Hardware**

10.1.8.1 **Centralized FMCC**

a) Each Remote site shall support interface to a minimum of 2 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.

10.1.8.2 **Standalone FMCC**

a) The system shall support interface to a minimum of 2 CCS-7 links expandable in steps of 2 links.

b) The system shall be able to handle up to 300 signaling links.

10.1.9 **Modularity**

10.1.9.1 The equipment shall have Redundant Processor configuration working in load-sharing basis or active and hot standby mode If load sharing mode is used and one of the processor fails, the other shall handle the full load and system may work in degraded performance mode.

Total system downtime shall be zero in both the configurations.

10.1.9.2 RAID arrangement may be used for secured data storage.

10.1.9.3 The configuration shall meet the processing, storage, input/output, networking requirements including ETHERNET and X.25 adapters.

10.1.9.4 The front-end terminals/user workstations shall be provided depending on the requirements.

10.1.9.5 All the data stored shall be protected against corruption and accidental loss.

10.1.9.6 The equipment, modems, routers, mediation devices, etc., for interfacing the FMCC to various systems shall be provided by System Supplier.

10.1.9.7 All interface connectors and cables shall be compatible with equipment in the switching/ other systems. No hardware change or augmentation of hardware shall be necessary in these systems.

10.1.9.8 System Hardware shall not pose any problem, due to changes in date and time caused by events such as changeover of millennium/century, leap year etc., in the normal functioning of the system.

10.2 Software Requirements

The software of FMCC shall cater for the functional requirements of fraud detection and analysis, interface to various systems and data formats of the inputs for analysis. Following clauses specify the software requirements for fraud detection and control as well as data acquisition from various systems through appropriate interfaces.

10.2.1 **Fault Tolerant Software :** The Software shall provide Automatic Switching 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 shall 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.

10.2.4 Software Rights along with source code shall be provided by the System Supplier for possible usage of the FMCC at more than one site at the discretion of Service provider.

10.2.5 The software shall be written in a High Level Language.

10.2.6 The software shall conform to the following characteristics:

i. The design of the software shall be such that the system is easy to handle both during installation and normal operations.
ii. The functional modularity of the software shall permit introduction of changes wherever necessary with least impact on other modules.
iii. It shall be open-ended to allow addition of new features.
iv. Adequate flexibility shall 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 shall provide sufficient checks to monitor the correct functioning of the system.
vii. Test programs shall include fault tracing for detection and localization of system faults.
viii. Facilities shall 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 $\pm$ 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. UPS and other power requirements are to be specified by the system supplier.

10.4 **Building**

10.4.1 It shall be possible to accommodate the equipment in buildings constructed to the following specifications.

Floor Loading	400 Kg/ Sq. M.
Clear Ceiling Height	2.9 Meter

10.4.2 Florescent lamps for general lighting to a level of 300 Lux are usually provided in the equipment rooms.

GLOSSARY

CDR	Call Detail Record
DAT	Digital Audio Tape
FMCC	Fraud Management and Control Centre
GR	Generic Requirements
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

Annexure I

Comments on draft standards for Generic Requirements(GR) "FRAUD MANAGEMENT AND CONTROL CENTRE (TEC 58110:2010)"

Name:

Organisation:

Contact Details:

S.No	Clause No	Clause	Comments	Other Remarks(if any)