Annexure-1

Airtel's Response to Consultation Paper on
The Telecommunication (Broadcasting and Cable) Services
Digital Addressable Systems Audit Manual dated March 29, 2019

At the outset, we wish to submit that the very objective of incorporating the provisions pertaining to the Audit of DPOs' Addressable Systems in the Interconnection Regulation, 2017 was to avoid the multiplicity of Audits caused by Broadcasters. Accordingly, the Interconnection Regulation has specified that DPO has to get its addressable systems audited once in a year. Therefore, to uphold the spirit of avoiding multiple audits, it should be ensured that there is no exploitation of the provisions of the Regulation regarding a challenge Audit that can be caused by Broadcaster even when DPO has been issued a positive report by the empanelled auditor. There should be valid justifications and reasons duly substantiated with data basis which the Broadcasters should be entitled to challenge the Audit.

Issues for Consultation:

Q1. Whether it should be mandatory for every DPO to notify the broadcasters (whose channels are being carried by the DPO) for every change made in the addressable system (CAS, SMS and other related systems)?

Response:

It should not be mandatory for a DPO to notify each and every change carried out on in its addressable or related systems to Broadcasters as the routine activities of the DPOs do not have any implications on the functioning of addressable systems. Moreover, as DPOs are liable to get their systems audited once in a year, there should be no apprehensions about such routine changes impacting the system functionality as any deficiencies in the system will automatically get highlighted in the annual Technical and subscription audits.

Q2. Whether the Laptop is to be necessarily provided by the Auditee DPO or the Audit Agency may also provide the Laptop? Please provide reasons for your comment.

Response:

Yes, the Laptop is to be necessarily provided by the Auditee DPO. Auditors should be allowed to use the laptop/PC provided by the DPO's only. All the data collected during the course of the Audit should be retained on the laptop provided by DPO. No raw/collected data should be allowed to be extracted from the PC. The same is necessary to ensure that no commercially sensitive data as well as other confidential data is taken out by the auditor in any form. Moreover, it has already been specified in the draft manual that DPO will save past audit data in PC provided by them in password protected folders which can be referred to by auditors in future. In case, the Auditors have any specific software requirements, the same should be notified to the Auditee well in advance at least 2 months prior to the scheduled Audit. Only in exceptional cases if it is explicitly agreeable to DPO, the auditor may be allowed to use its own laptop.

Q3. Whether the Configuration of Laptop vide Annexure 1 is suitable? If not, please provide alternate configuration with reasons thereof.

Response:

The configuration of Laptop suggested is fine.

Q4. Do you agree with the provisions regarding seeking of TS recording and ground sample information from IBF/ NBA for verification/ checking by the Auditor?-

Response:

We again hereby submit that necessary framework and arrangements need to be put in place to ensure that there are no unnecessary claims by Broadcasters to cause challenge Audits as this will unnecessarily increase operational burden on DPOs. In case a challenge audit is requested by a Broadcaster all necessary measures should be taken, including seeking TS recording and ground sample information from IBF/ NBA, to ascertain the validity of the claim so that unnecessary audit can be avoided.

Q5. Do you agree that Data Dump may be cross-checked with weekly data of sample weeks basis? If yes, do you agree with checking of random 20 % sample weeks? Please support your comments with justification and statistical information.

Response:

We hereby submit that checking of random 20% sample weeks' data dumps will be practically infeasible. The extraction of such huge data may put an additional load on the IT systems and this may result in interference with the routine activities or impact the customer experience or journey. For DTH operators who serve large number of customers, data dumps are of around 15-20 GB size per day. Therefore, significant time will be lost in retrieval of data dumps, In order to make it practically feasible, data dumps of maximum 5% sample weeks can be checked by auditors.

Q6. Do you agree with the proposed Data extraction methodology? If not, suggest alternates with reasoning thereof.

Response:

We agree that the dumps will be extracted by DPO personnel in front of Auditors. However, no Auditor should be allowed to get a direct access to DPOs systems. The same should be made explicitly clear in the Audit manual.

We would also like to emphasize that the DPO team shall run the queries for the data extraction from the dumps or otherwise in the presence of the Auditors and basis the Auditors requirements. Thus, there should not be any provision which allows auditors to have a direct access of any DPO's system or the need to disclose any admin/super admin login access. This is to ensure that the live systems of the DPO are duly protected and the confidentiality of the sensitive information is duly maintained.

Q7. Do you agree with verification and reporting of City-wise, State-wise and Head-end wise subscription report? Please provide supporting reasons/ information for your comment.

Response:

City-wise and State-wise data has got no relevance for settlement between DPO and Broadcasters. Large DPOs like DTH operators operate on Pan-India basis and there is no justification for seeking City-wise and State-wise data for audit purposes as it is not a part of reports provided by DPOs to broadcasters. The City wise and State wise data has no bearing on the payouts to be made by the DPO's to the Broadcasters. Further, this requirement does not owe its origin to any of the provisions of the new framework of TRAI. Such requirement being outside the ambit of the TRAI framework cannot be made part of the audit. Further, such data is commercially sensitive data, therefore, City-wise and State-wise information cannot be shared with Auditors for any kind of verification. We therefore, submit that we are not agreeable to this requirement and hence the same should be removed from all sections of the Audit Manual, wherever it is specified.

Q8. Do you agree with the tests and procedure provided for checking covert and overt fingerprinting? Provide your comments with reasons thereof?

Response:

Most of the STBs available in the market do not support covert type of fingerprinting. Therefore, the requirement of demonstrating covert type of fingerprinting should be made optional. If DPO is able to demonstrate overt type of fingerprinting then it should suffice the requirement as the end objective can be met with this as well

Also for the test pertaining to triggering of fingerprinting for five minutes, fingerprinting will be demonstrated on a pre-defined services or channel chosen by DPO.

Q9. Any other suggestion/ comments on the provisions or methodology proposed in the Audit Manual.

Response:

1. We reiterate that the principle of avoiding multiplicity of Audits should be upheld; therefore, the provision to revalidation of new head-end upon commercial launch will be an unnecessary exercise if the head-end has already been audited by auditor once by the auditor.

2. Any sort of modification logs (package composition change logs) cannot be provided since it is not feasible to be extracted from the system. Moreover, this is not relevant for the purposes of Audit and is also not asked in the audits being conducted by Broadcasters. Therefore, this requirement needs to be removed.

3. The Auditee DPO should be given at least 30 working days to give its comments on the draft report. Since the audit is significant and the scope of the audit is wide, there should be an adequate time to be provided to DPO to respond to the Audit Report.

4. As per the draft manual scrolling capability is to be demonstrated from CAS. In this regard, it is submitted that the scrolling capability will be demonstrated from either, the CAS or SMS and the associated peripheral systems. Since the end objective can be achieved with CAS or SMS, therefore, this flexibility should be allowed.

5. The requirement of providing compliance certificates should be applicable only for the set-top boxes which are currently being deployed in the network; not on the previous set-top boxes (which are not being deployed currently by operator). The requirement of providing certificates of the discontinued models of Set-top boxes will create logistic issues as some of the vendors may have already discontinued production completely.

6. Any mandate to audit records of last 2 years should not to be specified: In the draft audit Manual, there has been a requirement to furnish records of last 2 years and this requirement is specified under various clauses of the Manual. As the Authority is aware, the new regulatory framework has been implemented pursuant to which the entire ecosystem has undergone significant changes and a new regime is in place. Therefore, the requirement to audit last 2 years data will not serve any purpose as any data prior to the new regime cannot be subject to audit basis the provisions of the new framework. It is therefore, imperative and logical that the period and the data to be reviewed be limited to the period after the new framework has been implemented. Considering the huge volumes of data and the sensitivity of the data involved, any requirements for logs should also be restricted to on a sampling basis. Further, the data to be taken/examined during the audit should be strictly confined to the period for which audit is being conducted as this is an annual feature so 2 years requirement is not appropriate.

7. The Audit Manual also provides for physical verification of CAF/ SAF forms of customers activated in last 6 months with all customers entered in SMS. This requirement has no significance as the results of test subscribers is more than adequate to establish the veracity of the process. Therefore, the audit steps should be limited to test users cases only and the 6 months of all customers should be excluded from the audit steps owing to concerns of privacy and the fact that the requirement is overstretching and serves no purpose. (Page 31 point no.13 of Draft Audit Manual)

8. The extraction of customer data from SMS should be restricted to count and no other information concerning the identity and demographics of the customer; viz; name of the customer, Billing address, Installation address, Landline telephone number, Mobile telephone number, E-mail address, Channels, bouquets and services subscribed, Unique STB number should be allowed as the said information is confidential and the requirement of the audit can be effectively met with the count of the subscribers. (Page 31 point no.13 of Draft Audit Manual)