



भारतीय दूरसंचार विनियामक प्राधिकरण

Telecom Regulatory Authority of India



**‘Draft Telecommunication (Broadcasting
& Cable) Services DRM Based Digital
Addressable Systems Audit Manual’
for seeking comments of Stakeholders**

New Delhi
9th October 2026

World Trade Centre
4th, 5th, 6th & 7th Floor, Tower F, Nauroji Nagar
New Delhi-110029
Website: www.trai.gov.in

Inputs, comments or suggestions, if any, on the various clauses of the **Draft DRM Audit Manual**, may be sent to the Advisor (B&CS), Telecom Regulatory Authority of India, World Trade Centre, 4th, 5th, 6th & 7th Floor, Tower F, Nauroji Nagar, New Delhi – 110029, India, preferably by e-mail at advbcs-2@traai.gov.in, or to the Joint Advisor (B&CS) at jtadvbcs-3@traai.gov.in, in the format given below. Last Date of submitting comments is **30.10.2026** (three weeks from the date of issue of this Manual).

A. Comments on existing clauses of draft DRM Audit Manual

S. No.	Page no. of the Draft Audit manual	Clause No. of the draft Audit Manual	Do you agree with the Clause of the draft Audit Manual	If you do not agree with the proposed clause then provide suggested amended clause	Reasons with full justification of your response
1.					
2.					
3.					
...					

B. Comments on inclusion of any new clause in the draft DRM Audit Manual other than those already provided for

S. No.	Suggested New clause	Please indicate the page no. clause No. where it is to be inserted	Detailed Reason/ justification for the proposed amendment
1.			
2.			
3.			
...			

INDEX

S. No.	Contents	Page No.
1	Background & Introduction	1
2	Pre-signal or Compliance Audit	4
3	Scheduling of pre-signal or compliance audits	7
4	Scope of work under pre-signal/compliance audit	8
5	Documents requirements under pre-signal/compliance audit	10
6	Methodology to be adopted for pre-signal/compliance audit.	11
7	Procedure to be followed for inspection of Schedule X of the Interconnection Regulation Compliance • DRM requirements for SMS • DRM Requirements for conditional access /Encryption • Fingerprinting requirements for DRM • STB/unique consumer subscription requirements for DRM	13
8	Timelines under pre-signal/compliance audit	35
9	Subscription Audit	35
10	Scope of work under Subscription Audit	37
11	Documents requirements under Subscription Audit by auditor	40
12	Methodology to be adopted for Subscription audit	41
13	Procedure to be followed for inspection of Subscription audit	42
14	Scheduling of Subscription Audit	43
15	A. Timelines for completion of Subscription Audits B. Timelines for completion of both Technical and Subscription Audits	43
16	Data Extraction Procedure to be followed by auditor under compliance and subscription audit	44

S. No.	Contents	Page No.
17	Analysis and Verification of VC samples	45
18	Responsibilities in respect of Compliance and Subscription Audit A. DPO B. Broadcaster and C. Auditor	47
19	Minimum Laptop Configuration to be provided by DPO	56
20	Formats of Annexures and Reports 1. DRM Vendor Declaration (Annexure 1) 2. SMS Vendor Declaration (Annexure 2) 3. Compliance audit form (Annexure 3) 4. STB/User device Software Application Vendor Declaration (Annexure 4) 5. Certificate from provider/developer of software application installed in user device (Format as in Annexure 5). 6. Subscription Audit Form (Annexure 6) 7. Compliance Audit Report Format (Annexure 7) 8. Subscription Audit Report Format (Annexure 8) 9. Format of Infrastructure sharing to be filled in by Infrastructure provider (Annexure 9)	57

1. Background & Introduction

1.1 The Telecom Regulatory Authority of India (hereinafter referred to as "TRAI" or "the Authority") notified the regulatory framework for broadcasting and cable television services provided through Digital Addressable Systems (DAS) on 3rd March 2017. The framework strives to create a level playing field among stakeholders, ensure fair competition and foster the orderly growth of the broadcasting and cable TV sector. Pursuant to legal challenges before various fora, the framework came into effect from 29th December 2018. It comprises the following three instruments:

- (i) The Telecommunication (Broadcasting and Cable) Services (Eighth) (Addressable Systems) Tariff Order, 2017 ("Tariff Order, 2017");
- (ii) The Telecommunication (Broadcasting and Cable) Services Interconnection (Addressable Systems) Regulations, 2017 ("Interconnection Regulations, 2017");
- (iii) The Telecommunication (Broadcasting and Cable) Services Standards of Quality of Service and Consumer Protection (Addressable Systems) Regulations, 2017 ("QoS Regulations, 2017").

1.2 The Interconnection Regulations, 2017 has since been amended on several occasions, including on 30th October 2019, 1st January 2020, 11th June 2021, 22nd November 2022, 14th September 2023, 8th July 2024 and 5th February 2026 (the principal regulations, read with all amendments notified from time to time, are hereinafter referred to as the 'Interconnection Regulations'). Of these, the amendment notified on 14th September 2023, viz., the Telecommunication (Broadcasting and Cable) Services Interconnection (Addressable Systems) (Fifth Amendment) Regulations, 2023, inserted the Schedule X, prescribing Digital Rights Management (DRM) System Requirements applicable

primarily to IPTV-based distribution, covering (i) DRM requirements for subscriber management systems (SMS) used for IPTV services, (ii) DRM requirements for conditional access and encryption for IPTV services, (iii) DRM requirements for fingerprinting for IPTV services, and (iv) DRM requirements relating to unique consumer/subscription identification for IPTV services.

- 1.3 The 'Interconnection Regulations' cover the technical and commercial arrangements between Broadcaster and Distributor, for the provision of television services to consumers. A distinct and comprehensive DRM Audit Manual has not yet been formalized. The Authority has initiated preparatory measures towards its development, including the drafting of the Manual and the issuance of this draft Audit manual for seeking comments of stakeholders.
- 1.4 In the DAS based television services value chain, a broadcaster uplinks the signal of a pay television channel to satellite in encrypted form. The distributor receives the signal from the satellite and decodes it using the decoder provided by the broadcaster. After processing and merging the television channel signals of multiple broadcasters, the distributor encrypts the combined signal and retransmits it, either directly or through a Local Cable Operator (LCO), to the customer. The distributor may be a Multi-System Operator (MSO), a Direct to Home operator (DTH), a Head-end in the Sky operator (HITS), or an Internet Protocol Television (IPTV) operator. Where the distributor is an IPTV operator, the addressable system typically relies on a DRM architecture, which comprises of a DRM packager, one or more license servers, and associated key-management and entitlement systems, in place of, or alongside, a conventional Conditional Access System (CAS).
- 1.5 The 'Interconnection Regulations' provide a comprehensive framework for the audit of a distributor's addressable systems. Under Regulation 15(1), every distributor of television channels is required to get the

addressable systems of its distribution platform, including the SMS, CAS, DRM system and other related systems, audited once every year for the preceding financial year by an auditor empanelled by the Authority or M/s Broadcast Engineering Consultants India Limited (BECIL). The audit is intended to verify the correctness and completeness of the information contained in the monthly subscription reports furnished to broadcasters, and the audit report, along with all annexures, is required to be shared with each broadcaster with whom the distributor has entered into an interconnection agreement by 30th September every year. The distributor is also required to provide advance notice of the audit schedule to broadcasters, who may depute a representative to participate in the audit process for the limited purpose of providing inputs for verification. The obligation to undergo such audit is optional only for distributors whose active subscriber base on the last day of the preceding financial year does not exceed thirty thousand subscribers, subject to the conditions prescribed in the Regulations.

Further, Regulation 15(1A) provides for the imposition of financial disincentives on distributors that fail to get the prescribed audit conducted within the stipulated time.

The Regulations also provide mechanisms enabling broadcasters to seek further scrutiny where concerns arise regarding significant inadequacies or discrepancies in such audit report. Under Regulation 15(2), a broadcaster that identifies significant inadequacies or discrepancies in an audit report received under Regulation 15(1) may submit its observations, along with supporting documents, to the distributor within the prescribed period. Such observations are required to be examined by the concerned auditor, who may issue an updated audit report. Further, if the broadcaster finds that its observations have not been addressed completely, it may make a representation before the Authority with its specific observations and supporting documents, if

any, within thirty days of receipt of updated audit report. The Authority may permit the broadcaster to get the audit conducted from any of the auditors empanelled by the Authority, or M/s Broadcast Engineering Consultants India Limited, to verify the inadequacies/discrepancies pointed out by the broadcaster and the cost of such audit shall be borne by the broadcaster.

In addition, Regulation 15(2A) permits broadcasters to cause an audit of a distributor's addressable systems at their own cost in cases where a distributor that is obligated to undergo audit under Regulation 15(1) fails to furnish the audit report by 30th September. Where the audit under Regulation 15(1) is optional because the distributor's subscriber base does not exceed the prescribed threshold, broadcasters may jointly cause such an audit after informing the distributor in writing. Any audit undertaken under these provisions is subject to the limitations and timelines specified in the Regulations. Further, Regulation 15(2B) provides that where an audit conducted under Regulation 15(1), Regulation 15(2) or Regulation 15(2A) reveals discrepancies in subscriber declarations, the resulting payment liabilities may be settled in accordance with the interconnection agreement, and where the addressable system is found not to comply with the requirements of Schedule III, Schedule X, or both (as applicable), the broadcaster may disconnect signals after giving three weeks' written notice to the distributor.

- 1.6 The Authority undertook a broader review of audit ecosystem, in order to strengthen it and make it more rigorous. Accordingly, the conditions for empanelment of auditors were revised to enhance accountability of auditors. The Seventh Amendment to the Telecommunication (Broadcasting and Cable) Services Interconnection (Addressable Systems) Regulations, 2026, was notified on 5th February 2026. Subsequently, the Telecommunication (Broadcasting and Cable) Services Digital Addressable Systems Audit Manual, 2026 issued on

10th March 2026. The Audit Manual sets out, in considerable detail, the scope of work, documentation requirements, data-extraction methodology and clause-wise audit procedure for verifying compliance with Schedule III i.e., for CAS/SMS/STB based addressable systems. It does not contain a corresponding clause wise audit procedure for Schedule X. Stakeholders, including, IPTV operators, broadcasters and auditors, have given inputs through various forums that a similar audit manual is required for DRM based systems.

- 1.7 To address this gap, the Authority in consultation with M/s Broadcast Engineering Consultants India Limited (BECIL) has prepared a draft DRM Audit Manual, setting out a dedicated audit methodology for Schedule X. In preparing the draft manual, the infrastructure-sharing guidelines for DPOs issued by the Ministry of Information and Broadcasting (MIB) have also been considered.
- 1.8 The draft DRM Audit Manual so prepared is being published for seeking the comments of the stakeholders. Any comments should be supported with reasoning and explanation. Stakeholders should provide the necessary evidence/data points to support their comments. Where an alternate formulation of any paragraph or clause of the draft audit manual is proposed, the comment should set out the exact alternate language proposed and the reasons for the proposed change.
- 1.9 This audit manual addresses issues related to DAS audits in terms of Regulations 10 and 15 of the Interconnection Regulations 2017.
- 1.10 During the course of time, necessity of modifications in this manual may arise due to technological/techno-commercial changes, market development and changes in the systems, etc. Accordingly, this audit manual may be reviewed if required. The Authority may notify such modifications which shall come into effect from the date as prescribed in the notification.

- 1.11 The Audit Manual is proposed as a guidance document for stakeholders. This manual does not supersede any provision(s) of the extant regulations. In case of any discrepancy between the provision of the 'Interconnection Regulations', other extant Regulations or Tariff Order and the Audit Manual, the provisions as per the regulations/tariff Orders shall prevail.
- 1.12 The audits provisioned under the 'Interconnection Regulations' are broadly divided into two categories (i) pre-signal or compliance audit and (ii) subscription audit. As per the Regulation, the DPO and broadcasters can get the audit conducted either by any agency empanelled by TRAI or M/s. Broadcast Engineering Consultants India Limited (BECIL). The list of auditors empanelled by TRAI is available on TRAI's website: www.traigov.in. The broad scope of work to be covered under these audits, procedure for conduct and other necessary information is mentioned in the sections below.

2. DRM Pre-signal or Compliance Audit

- 2.1 The audit will be called pre-signal audit if it is carried out before the content acquisition by the Distribution Platform Operator (DPO) from respective broadcaster. It may be noted that pre-signal/compliance audit for DRM based systems will be carried out as per Schedule X of the 'Interconnection Regulations'.
- 2.2 In accordance with the sub-regulation (6) of regulation 10, every distributor of television channels before requesting signals of television channels from a broadcaster shall ensure that the DRM based addressable systems to be used for distribution of television channels meet the requirements as specified in the Schedule X of the 'Interconnection Regulations'. For ensuring the same, DPO can get the

pre-signal audit conducted either by any agency empanelled by TRAI or BECIL.

2.3 It is clarified here that before requesting signals of television channels, it is not mandatory for DPO to get its DAS system audited from any auditor empanelled by TRAI or BECIL as per Schedule III or X or both (as applicable) under sub-regulation (6) of regulation 10 of the 'Interconnection Regulations'. However, every distributor of television channels shall ensure that before requesting signals of television channels from a broadcaster, the addressable systems to be used for distribution of television channels meet the requirements as specified in the Schedule III or X or both (as applicable) of the 'Interconnection Regulations' and the DPO may provide its declaration in writing to broadcaster regarding compliance to Schedule III or X or both (as applicable) of 'Interconnection Regulations' along with below mentioned documents for requesting signals.

- CAS/DRM certificate provided by vendor.
- SMS certificate provided by vendor.
- STB/Software Application in user device certificate provided by vendor.
- BIS compliance certificate. (If applicable).
- Software Application certificate (If applicable).

2.4 Sub-regulation (7) of Regulation 10 of the 'Interconnection Regulations' specifies that if a broadcaster, without prejudice to the time limit specified in sub-regulation (2) of regulation 3, is of the opinion that the addressable system, being used by the distributor for distribution of television channels, does not meet the requirements specified in the Schedule III or X or both (as applicable) of the 'Interconnection Regulations', it may, cause audit of the addressable system of the distributor by any auditor empanelled by the Authority or M/s.

Broadcast Engineering Consultants India Limited (BECIL), and provide a copy of the report prepared by the auditor to the distributor. However, it is important to note the proviso to the sub-regulation (7)¹ of Regulation 10, before instituting such audit by the broadcaster.

- 2.5 The proviso to the said Regulations provides for the case where the system of the distributor has been successfully audited (with full compliance) during the last one year by any auditor empanelled by the Authority or M/s. Broadcast Engineering Consultants India Limited (BECIL). In such case, if the distributor provides the report of the Audit (conducted during the preceding one year) to the broadcaster, then the broadcaster shall not cause pre-signal audit, unless the configuration or the version of the addressable system has changed after the issuance of the report by the auditor.
- 2.6 Therefore, the pre-signal audit may also be commissioned by the broadcaster to satisfy itself that the distributor, to whom it is likely to provide television signal, meets the DRM system requirements as per Schedule X of the 'Interconnection Regulations'. As such the audit fees for such audit will be borne by the broadcaster. In case(s) of pre-signal audit by a broadcaster only technical audit is required to be conducted.
- 2.7 Annual Compliance Audit: As per sub-regulation (1) of Regulation 15 of the 'Interconnection Regulations', every distributor of television channels shall get addressable system of its distribution platform, such as Subscriber Management System, Conditional Access System, Digital Rights Management System, and other related systems audited once every year, for the preceding financial year. The annual audit caused by

¹ Proviso to sub-regulation (7) of Regulation 10 "Provided that unless the configuration or the version of the addressable system of the distributor has been changed after issuance of the report by the auditor, the broadcaster, before providing signals of television channel shall not cause audit of the addressable system of the distributor if the addressable system of such distributor has been audited during the last one year by M/s. Broadcast Engineering Consultants India Limited, or any other auditor empanelled by the Authority and the distributor produces a copy of such report as a proof of conformance to the requirements specified in the Schedule III or Schedule X or both, as the case may be."

distributor shall include the audit to validate compliance with the Schedule X of the 'Interconnection Regulations' and the subscription audit, as provided for in the 'Interconnection Regulations'. The above annual compliance audit will also be applicable in case of infrastructure sharing.

2.8 Once an interconnection agreement has been signed between a Broadcaster and DPO, if any changes, modification and alterations are made to the configuration or version of the addressable system (DRM, SMS and other related systems) of the DPO and/or distribution network of DPOs ("changes"), then these should be notified within seven (7) days to the relevant broadcasters. DPO shall provide an undertaking that the changes do not in any way compromise the system and the set-up and all the equipment including software meets the statutory compliance requirements.

2.9 In order to avoid any dispute, in case of changes mentioned below in Digital Addressable System, the broadcaster can cause the audit under sub regulation (7) of regulation 10 of the 'Interconnection Regulations', before providing signals of television channels to DPO. It may also be noted that these changes are also required to be formally informed to broadcasters by DPO within 7 days from the implementation date of these changes:

- a) Addition/Deletion of SMS*
- b) Change in the SMS version w.r.t last audited SMS*
- c) Addition/Deletion of DRM*
- d) Change in the DRM version w.r.t last audited DRM*
- e) Deployment of new type of STBs/software application in user device by DPO which were not audited earlier.*
- f) In case any DPO opts for infrastructure sharing as and when permitted (either provider or seeker) or shifts from one DPO to another for infrastructure sharing.*

2.10 Further, the STB or software application linked to unique consumer subscription deployed should be capable of supporting content decryption, decoding and DRM license evaluation. The 'Unique consumer subscription' mentioned in Schedule X refers to the software application installed in the user device by a DPO providing IPTV services to a consumer and which performs all the functions of an STB linked to the unique consumer subscription.

2.11 Subject to conformance to Regulation 11 of the 'Interconnection Regulations', the distributor may extend territory of interconnection agreement by giving a written notice to the broadcaster providing at least 30 days to the broadcaster. In such cases, the distributor shall also inform the broadcaster formally after 7 days of actual extension of the territory.

3. Scheduling of Pre-signal or Compliance Audits

3.1 There are no specific timelines for conducting the pre-signal audits. Pre-signal audit can be conducted at any stage whenever DPO wants to ensure that the DAS system is in compliance as per the 'Interconnection Regulations'. As mentioned earlier, as per sub-regulation (1) of Regulation 15, the annual audit caused by a distributor using DRM systems shall include the audit to validate compliance with the Schedule X of the 'Interconnection Regulations' and the subscription audit, as provided for in the 'Interconnection Regulations'. Further, every DPO shall get addressable system of its distribution platform, audited once every year, for the preceding financial year, by an auditor, to verify the information contained in the monthly subscription reports made available by the distributor to the broadcasters, and the distributor shall ensure that the relevant audit report, including all annexures, is shared with each broadcaster with whom it has entered into an interconnection agreement, by the 30th September every year.

- 3.2 Broadcaster can schedule the audit of DPO by selecting an auditor empanelled by the Authority or BECIL for conducting compliance audit as per provisions of sub-regulation (2) and (2A) of Regulation 15 of the 'Interconnection Regulations' (or in case of pre-signal audit, after taking into consideration the proviso to sub regulation 7 of Regulation 10).

4. Scope of work under pre-signal/compliance audit

- 4.1 Perform walk-through of all the headend(s) and perform all audit checks as mandated in TRAI Regulation.
- 4.2 Obtain Headend diagram and validate the equipment installed in the headend(s).
- 4.3 Perform checks on IP configuration to confirm and identify live and proxy servers. This shall include IP credentials of all the servers.
- 4.4 Take the declaration of DPOs regarding the IRDs deployed in the headend including serial/VC numbers. The Auditor shall check all the IRDs +VCs deployed by the DPO during the audit. The checking may preferably be done during lean hours. The auditor shall ensure that there is no disruption of the live service of DPO².
- 4.5 Obtain record of Program Specific Information/Service Information (PSI/SI) server to confirm Electronic Programme Guide (EPG), Logical Channel Number (LCN) etc. details.
- 4.6 Check PSI/SI server that it has EPG push capability.

² It is time consuming to take the inventory list from each broadcaster, and this results in unnecessary delays. The IRDs are deployed in the headend which are issued by broadcasters. These IRDs are audited and details are furnished in the audit report. After the issuance of audit report, broadcasters can crosscheck these IRD details and can reconcile the same with DPO in case of any dispute.

- 4.7 Confirm insertion of watermarking network logo for all channels from encoder end. Only the encoders deployed after coming into effect of the Telecommunication (Broadcasting and Cable) Services Interconnection (Addressable Systems) (Amendment) Regulations, 2019 (7 of 2019) dated 30th October 2019 [hereinafter called Amendment Regulations 2019] shall support watermarking network logo for all pay channels at the encoder end. In case of infrastructure sharing, the requirement in respect of watermarking for insertion of network logo for all pay channels at only encoder end shall be applicable for infrastructure provider. The infrastructure seeker shall provide network logo through STB/middleware. However, preferably only two logos, that is, of only broadcaster and last mile distributor shall be visible at customer end.
- 4.8 Walkthrough and understand the customer acquisition process and verification of applicable forms such as sample Customer Acquisition Form (CAF) and Pack Authorisation Form (PAF) forms available with DPO.
- 4.9 Verification of compliance of Schedule X of the 'Interconnection Regulations' of the DPO's DAS System (DRM, Fingerprinting and STB/software application in user device) as per procedure mentioned in section 7 of the Audit Manual.
- 4.10 Data Extraction from DRM and SMS should be carried out as per requirements specified in Schedule X of the 'Interconnection Regulations'. Procedure and method of data extraction is specified in the section 7 and section 16 of the Audit Manual.
- 4.11 Report the channels found running in unencrypted or analogue mode on the day of Audit.
- 4.12 Analysis and verification of VC samples/Unique Consumer Subscription (software application installed in the user device) /device

provided by broadcasters may also need to be covered under scope of work. However, the procedure to be followed for carrying out such analysis and verification are mentioned separately in the section 17 of the Audit Manual.

4.13 The above scope of work will also be applicable in case of infrastructure sharing between multiple DPOs.

- In the course of auditing an infrastructure seeker, the scope of review shall be limited to the seeker's DAS and the elements obtained through infrastructure sharing arrangements from the infrastructure provider³.
- When auditing an infrastructure provider, the audit shall encompass all DAS elements under its ownership and the elements shared with the infrastructure seeker through infrastructure sharing arrangements.

For ease of doing business and audit, it would be advisable for infrastructure providers and seekers to conduct audit of their DAS system jointly (provider + seeker) especially when they are sharing SMS.

In the case of sharing of SMS, broadcaster(s) can conduct joint and simultaneous audits covering all elements of all the DPOs sharing the infrastructure, as per the 'Interconnection Regulations', if required.

5. Documents required under pre-signal/ Compliance audit

³ Audit may be restricted to infrastructure sharing seeker and related elements of the infrastructure sharing provider. Justification for the same is that the other elements under audit of infrastructure sharing provider such as DRM, SMS, mux, encoders, etc. which are not related to Infrastructure sharing seeker will result in additional time and resources of the stakeholders that are involved in this process without any material effect on the audit.

- 5.1 Valid DAS/IPTV permission issued by Ministry of Information and Broadcasting (MIB).
- 5.2 BIS certificates for all makes & models of DRM based STB deployed by DPO after September 2023.
- 5.3 Certificate from all the DRM vendors (Format as in **Annexure 1**).
- 5.4 Certificate from SMS vendors (Format as in **Annexure 2**).
- 5.5 Block Schematic diagram of Head-end including DRM and SMS.
- 5.6 Signed and stamped copy of compliance audit form as per **Annexure 3**.
- 5.7 Certificate from STB vendor (Format as in **Annexure 4**).
- 5.8 Certificate from provider/developer of the software application installed in user device (Format as in **Annexure 5**).
- 5.9 Signed and stamped copy from Infrastructure Provider (If applicable) as per **Annexure 9**.
- 5.10 List of all the decoder along with Box serial no. or CAM module serial no. and VC serial numbers deployed in the Headend by the DPO⁴.
- 5.11 It may be noted that in case system generated reports captures all the field specified in the above declaration format, then the auditor may accept such system generated reports⁵.

⁴ Some DPOs receive broadcasters' signal through decoders provided by them and some DPOs use PIRD with CAM to receive the signals. Further, it is time consuming to take the inventory list from each broadcaster, and this results in unnecessary delays. The IRDs are deployed in the headend which are issued by broadcasters. These IRDs are audited and details are furnished in the audit report. After the issuance of audit report, broadcasters can crosscheck these IRD details and can reconcile the same with DPO in case of any dispute.

⁵ It has been brought to the notice of TRAI that sometimes auditors insist on certain specific formats which suit their reporting requirements. It creates a problem for DPOs whose audits are conducted by different auditors to provide such specific reports. This amendment will help to address this issue.

6. Methodology to be adopted for pre-signal/ Compliance Audit

- 6.1 The audit either will be caused by the DPO or by the Broadcaster by selecting one of the audit agencies empanelled by TRAI or BECIL.
- 6.2 Once the audit is scheduled, the DPO will immediately inform concerned broadcasters with whom it has entered into an interconnection agreement, at least thirty days in advance, the schedule of audit and the name of the auditor. The broadcasters will then arrange to provide VCs (if any) for verification during audit and will share the same with Auditors before the conduct of audit.
- 6.3 After the appointment by DPO or broadcaster, auditor will immediately ask DPO whether DPO has any objections regarding usage of its laptop for the conduct of audit.
- 6.4 If DPO has objections and wants to provide its own laptop for conduct of audit, then auditor need to convey its requirement of software or any other tool required during the conduct of audit.
- 6.5 The auditor will also share the documents requirements with DPO as specified in section 5 of the audit manual.
- 6.6 The minimum configuration requirement of laptop is mentioned in the section 19 of audit manual which should be provided by DPO to auditor. DPO is free to provide laptop of higher configuration also.
- 6.7 During the audit, auditor should carry out all the checks/verification as mentioned under section 4 (scope of work under pre-signal/compliance audit) at all head ends of DPO where the DRM and SMS servers are installed.

- 6.8 The audit for compliance to Schedule X of the Interconnection Regulations should be carried out by auditor as per procedure specified in section 7 of the Audit Manual.
- 6.9 The data extraction from DRM and SMS under compliance audit should be carried out as per section 7 of the Audit Manual.
- 6.10 The auditor will prepare the pre-signal/compliance audit report as per format provided in **Annexure 6** of the Audit Manual.
- 6.11 After the completion of audit, auditor will submit the copy of the audit report to DPO only if the audit is caused by DPO. It should be the responsibility of DPO to share the audit report with broadcaster whenever such requests are made (in case of pre-signal audit) or as specified in regulation 15.
- 6.12 If the audit is caused by the broadcaster, then the auditor will share the audit report copies both with broadcaster as well as DPO.
- 6.13 In case the audit report is non-compliant to the Interconnection Regulations then action may be taken as per sub-regulation (2B) of Regulation 15 of the 'Interconnection Regulations'.

7. Procedure to be followed for inspection of Schedule X of the 'Interconnection Regulations'

A. DRM and SMS requirements as per Schedule X of 'Interconnection Regulations'

Note: It may be noted that all simulations tests on STBs/unique consumer subscription (software application in user device that has been deployed and activated by the DPO) should be carried out on those STB models/unique

consumer subscription post coming into effect of the Schedule X in amendment to 'Interconnection Regulations' in September 2023.

SMS and DRM should have capability to meet all the requirements of each distributor as specified in schedule X of the 'Interconnection Regulation'. Further, separate instances should be created for each distributor using shared SMS/DRM and the data between two or more distributors must be segregated in such a manner that entity wise reconciliation should be possible to be carried out between SMS and DRM.

"Note: A unique consumer subscription shall represent an individual subscription availed by a consumer for accessing IPTV services. In the IPTV ecosystem, consumer access is increasingly being enabled through software applications installed on consumer devices in place of conventional Set Top Boxes (STBs). Accordingly, where a software application deployed by a DPO on a consumer device performs the core functionalities ordinarily associated with an STB, including but not limited to content decryption, content decoding, and Digital Rights Management (DRM) licence evaluation, in such cases 'unique consumer subscription' contained in Schedule X refers to such an application.

TABLE 1: DRM REQUIREMENTS FOR SMS

S. No.	DRM requirements for SMS	Audit Procedure
1	There shall not be any data mismatch between DRM and SMS. Maximum mismatch based on subscriber base may be allowed as mentioned below: (1) Must be less than 0.20% for subscriber base up to 100000 subs (0 to 200 for subscriber base of up to 100000) (2) Must be less than 0.04% for subscriber base up to	• Reconciliation needs to be carried out by the auditor for identifying the data mismatch between the DRM data and SMS data. • The reconciliation needs to be carried out on the 'as on date data' (during the conduct of audit) for verification. • The comparison table needs to be mentioned in the audit report.

	1000000 subscribers (0 to 400 for subscriber base of up to 1000000) (3) Must be less than 0.01% for subscriber base above 10000000 subscribers (0 to 1000 for subscriber base of up to 10000000) The data between both the systems shall be reconciled on a monthly basis. The reconciliation report shall be stored along with the system data for a minimum of three years or at least three audit cycles, or as per Schedule X whichever is later.	
2	Password Policy Creation for Users: SMS shall have a defined password policy, with minimum length criteria and composition (upper and lower-case characters, numeric, alphabets or special characters), forced password changes or any other appropriate mechanisms or combinations thereof or alternatively user account has to be locked/paired to the Mac Id of the set top box (STB) /unique consumer subscription⁶ or the customer premises equipment (CPE)/device.	• Auditor is required to check and validate the password policy creation of the IPTV user to be in line with the schedule X requirement by conducting a simulation test on the dummy customer.
3	After-Sales Service Support: The required software and hardware support should be available to the distributor of the television channels' installations from the SMS vendor's support teams located in India. The support	• Declaration to be provided by the SMS vendor.

⁶ The 'Unique consumer subscription' mentioned in Schedule X refers to the software application installed in the user device by a DPO providing IPTV services to a consumer and which performs all the functions of an STB linked to the unique consumer subscription.

	should be such as to ensure the SMS system with 99.99% uptime and availability. The systems should have sufficient provisions for backup systems to ensure quality of service and uptime	
4	All activation and deactivation of STBs/unique consumer subscription shall be done in such a way that SMS and DRM are always integrated and synchronized on real time basis.	• Simulation tests to be done during audit for verification of compliance.
5	Necessary and sufficient methods shall be put in place so that each activation and deactivation of STBs/unique consumer subscription is reflected in the reports generated from the SMS integrated with the DRM and vice versa	• Auditor to conduct simulation tests on the dummy customers regarding activations/deactivations and generate reports from DRM and SMS for compliance.
6	DRM and SMS should be able to activate or deactivate services and/or STBs/unique consumer subscription of the subscriber base of the distributor within 24 hours.	• Auditor to conduct simulation tests on the dummy customers for compliance.
7	The SMS shall be independently capable of generating, recording, and maintaining logs, for the period of at least immediately preceding three (3) consecutive years, corresponding to each command executed in the SMS including but not limited to activation and deactivation commands.	• Declaration to be submitted by the SMS vendor for compliance. • Auditor to check and record data availability in SMS in its audit report.
8	The SMS should be computerized and capable of recording all logs including information and data concerning the subscribers such as:	• Auditor to conduct simulation test on dummy/test subscribers in SMS for verification of compliance.

	(a) Unique customer identification (ID) (b) Subscription contract number (If applicable) (c) Name of the subscriber (d) Billing address (e) Installation address (f) Landline telephone number (g) Mobile telephone number (h) E-mail address (i) Channels, bouquets and services subscribed (j) Unique STB number/unique consumer subscription ID attached to a specific unique MAC ID. (k) Unique VC number or MAC ID.	
9	The SMS should be capable of: (a) Viewing and printing of historical data in terms of the activations and the deactivations of STBs/unique consumer subscription. (b) Locating each and every STB/unique consumer subscription and VC/MAC ID installed at city and state level. Generating historical data of changes in the subscriptions for each subscriber and the corresponding source of requests made by the subscriber.	• Auditor to conduct simulation test on dummy/test subscribers in SMS for verification of compliance.
10	The SMS should be capable of generating reports, at any desired time including about:	• Auditor to conduct simulation test on dummy/test subscribers

	(a) The total number of registered subscribers. (b) The total number of active subscribers. (c) The total number of temporary suspended subscribers. (d) The total number of deactivated subscribers. (e) List of blacklisted STBs/unique consumer subscription in the system. (f) Channel and bouquet wise monthly subscription report in the prescribed format. (g) The names of the channels forming part of each bouquet. (h) The total number of active subscribers subscribing to a particular channel or bouquet at a given time. (i) The name of a-la carte channel and bouquet subscribed by a subscriber. (j) The ageing report for subscription of a particular channel or bouquet.	in SMS for verification of compliance. • Sample reports/screenshots may be annexed with the auditor report.
11	The distributor shall ensure that the SMS vendor has the technical capability in India to maintain the systems on 24×7 basis throughout the year.	• SMS Vendor should submit its declaration for this requirement.
12	DPO shall declare the details of the DRM and the SMS deployed for distribution of channels. In case of deployment of any additional DRM/SMS, the same	• This requirement is a communication which is to be communicated prior by the DPO to the broadcasters. Hence, during the annual audit the

	shall be notified prior to commissioning of the system, to the broadcasters by the distributor.	auditor may confirm that this has been complied to by the DPO.
13	If there is active infrastructure sharing (as and when permitted by MIB) then, DPO shall declare the sharing of the DRM and the SMS deployed for distribution of channels. In case of deployment of any additional DRM/SMS, the same should be notified to the broadcasters by the distributor.	This requirement is a communication which is to be communicated prior by the DPO to the broadcasters. Hence, during the annual audit, the auditor may confirm that this action has been completed by the DPO. Accordingly, the same may be recorded in the audit report.
14	SMS shall have a provision to generate synchronization report, with date and time, with the minimum fields as listed below: (a) STB/unique consumer subscription Number (or in case of card-less system, chip ID or MAC ID number of the STB) (b) Product Code pertaining to à-la-carte channels and bouquets available on the platform (c) Start Date of entitlement (d) End Date of entitlement (e) Status of STB/unique consumer subscription (active/Inactive)	- Auditor is required to generate the report from SMS and check whether the details available in the report are as per requisite compliance of schedule X. - Sample pages/extract of the report generated may be annexed with the audit report.
15	The file output of DRM shall be processed by SMS system to compare and generate a 100% match or mismatch error report.	- Auditor is required to generate/extract the DRM and SMS data and reconcile it as per Sr. No. 1 of this table. - Observation of this analysis should be recorded in the audit report. The analysis should include STB/VC present/Active

		in SMS and not in DRM and vice versa
16	Channel/Bouquet management: SMS shall, in synchronization with DRM on real time basis, support the following essential requirements: (a) Create and manage relevant product ID for all channels and bouquets along with the relevant details such as name, tariff, broadcaster, or DPO bouquet, etc. (b) Manage changes in the channel/bouquet, as may be required, from time to time. (c) Link the Products IDs for à-la-carte channels and bouquets (Single and Bulk) created in DRM with the product information being managed in SMS, for smooth working of SMS and DRM integration. (d) Management of historical Data of Product name, i.e., Broadcasters (name), maximum retail price (MRP), distributor retail price (DRP).	• Auditor is required to extract the package composition data from DRM and SMS and check whether the same reconcile with each other. • To check whether the bouquet management provisions are available in SMS and DRM.
17	Network Capacity Fee (NCF) Policy Creation: SMS shall support all NCF related requirements mandated by the applicable tariff order.	• Auditor to check whether NCF provisioning is available in SMS.
18	Bill/Invoice Generation: SMS shall be capable of generating proper subscriber bill/invoice with explicit details of NCF charges, pay channels charges	• Auditor to check whether the SMS is capable of generating the Bill/Invoice to customers with prescribed details.

	(with clear itemized details of à-la-carte channel cost and bouquet costs), rental charges for STB/unique consumer subscription (if any), other applicable charges, including Goods and Services Tax (GST).	Sample bills (masking personal information of customers) may be enclosed with the audit reports.
19	Management of Logs: (a) SMS shall have the facility to provide user detail logs with the ID of users on each login event. (b) SMS shall have the provision of generating the user activity log report to enable tracking users' work history. It shall not be allowed to delete the records from the log. (c) All logs shall be stamped with date and time and the system shall not allow altering or modifying any logs. (d) The logs shall be maintained for a period as specified in Schedule X or at least three audit cycles, whichever is later. (e) Channel subscription report: SMS shall be able to provide broadcaster wise total counts of monthly subscribers of channels including both à la carte and bouquet subscriptions as per format that may be prescribed by TRAI. (f) DRM and SMS should be running on separate and independent servers.	• Auditor to check whether SMS has the ability or provisions for the Log management as required below: ○ User details logs of each login event of IPTV. ○ Activity logs report of users watching IPTV services along with history. ○ Date and time stamp on each and every logs. ○ Logs are available of the minimum period three years or the date installation/deployment of SMS. ○ SMS capability to generate the MSR Reports. ○ To check whether the SMS and DRM are running on independent servers. ○ Sample SMS Reports/logs/extracts may be annexed with the audit report.

20	SMS Database and tables: (a) There shall not be any active unique subscriber outside the database tables declared by the Vendor (b) SMS shall not provide an option to split SMS database or for creation of more than one instance. (c) SMS shall have the provision to enable or disable channel (à-la-carte channel or bouquet of channels) selection by subscribers either through website or an application through interface provided by the distributor platform operator. (d) SMS shall be capable of capturing the following information required for audit or otherwise: (i) Bouquet à la carte status change history (ii) Bouquet composition change history (iii) Change in status of connection (primary to secondary and vice versa)	• SMS vendor will provide the declaration for compliance • SMS vendor/DPO will show case all the database tables to the auditor to check and ensure that no subscriber is present outside the database tables. • No of SMS instances and any split databases will be checked by the auditor and record the same in its audit report. • Provision to enable or disable channel (à-la-carte channel or bouquet of channels) selection by subscribers either through website or an application will be checked by the auditor during simulation testing. • Auditor to check SMS capability to capture the following information: ◦ Bouquet à la carte status change history ◦ Bouquet composition change history • Change in status of connection (primary to secondary and vice versa)
21	SMS shall be accessed through a Firewall	• Auditor to check and verify the firewall deployed by the vendor/DPO for SMS.
22	STB/unique consumer subscription and MAC ID shall be paired from the SMS to ensure security of channel (applicable for DRM with pairing facility).	• Auditor to check and verify the provisioning during the simulation testing. (applicable for IPTV system where STB no/ unique consumer subscription (for Software application

		deployed by a DPO in user device) are paired with Mac ID)
23	The SMS shall be capable of individually addressing subscribers, for the purpose of generating the reports, on channel by channel and STB / unique consumer subscription by STB/unique consumer subscription basis.	• Auditor to check and verify the provision during the audit.
24	SMS should have a facility to carry out monthly reconciliations of channels/a-la-carte and bouquet (with their respective ID created in SMS with DRM) and the variance report should be available from the DRM and SMS logs and made available during audits.	• Auditor is required to generate/extract the DRM and SMS data and reconcile it as per Sr. No. 1 of this table. • Observation of this analysis should be recorded in the audit report.
25	SMS should have a provision of generating the following reports pertaining to STB/unique consumer subscription/MAC ID.: (a) Whitelist of STB/unique consumer subscription /MAC ID along with active/inactive status (b) Faulty STB/unique consumer subscription/MAC ID – repairable and beyond repairable (c) Warehouse fresh stock (d) In stock at local cable operator (LCO) end (e) Blacklist (f) Deployed with activation status (g) Testing/demonstration STB/unique consumer subscription/MAC ID with	• The auditor to take a written confirmation on this from the DPO/SMS vendor and record the same in audit report. • Sample SMS reports may be annexed with the audit reports

	location.	
26	Audit-related requirements: SMS should have the capability to capture below-mentioned information that may be required for audit and otherwise: (a) Subscriber related: (i) Subscriber contact details change history (ii) Connection count history (iii) Transition of connection between Disconnected /Active/Temporary Disconnected (iv) Subscription change history (b) Product (Bouquet/à-la-carte channel) related: (i) Broadcaster à-la-carte relation (ii) Bouquet name change history (iii) À la carte name change history (iv) Bouquet/à-la-carte channel rate change history (c) STB/unique consumer subscription related: (i) Change in location history (ii) Change in status (Active/ Damaged/ Repaired/ Replaced)	• Auditor to check and verify the provision/ ability of SMS to capture these requirements.
27	User Authentication: SMS should have the capability to authenticate its subscribers through registered mobile number (RMN) through one-time password (OTP) system.	• Auditor are required to verify the same during simulation testing. (Applicable only for OTP based user authentication). Note: RMN and Email id should be uniquely mapped for each user registered in the SMS system. It

		means the unique user should have unique RMN and email Ids.
28	SMS should have the provision to support the following additional requirements: (a) List of à-la-carte channels and bouquets, digital Headend (DHE): Provision to support/ Sub-Headend-wise list of à-la-carte channels and bouquets, in sync with the list available in DRM. (b) Product (à-la-carte channels and bouquets)-wise Renewal and Reversal setting for the Subscriber Account: Provision to allow renewal of a product to a subscriber after the expiry date of a product, and provision to auto-calculate and refund the amount to a subscriber if he discontinues a product midterm. These requirements may be configurable on selective products, as required by the DPOs as per their business plans. (c) Product (à-la-carte channels and bouquets)-wise Reversal setting for LCO Account: Provision to calculate and refund the amount due to LCO, if he or the subscriber discontinues a product midterm. Product (à-la-carte channels and bouquets) Tenure-wise LCO and Subscriber Discount Scheme/Free Days Scheme: Provision to create Discount Scheme and Free-day	• Auditor to check and verify the provision.

	scheme for LCO and Subscriber, based on the duration (Tenure) of the product subscription. (d) Calendar/Activity Scheduling: Provision to auto-schedule activities like STB/unique consumer subscription activation/deactivation, à-la-carte channels and bouquets addition/removal, channel/bouquet composition modification, etc. (e) Bulk Channel/Bouquet Management: Provision to perform bulk activity of à-la-carte channels and bouquets addition and removal on all or a designated group of STBs/unique consumer subscription. (f) Token-number-based reports: Provision to download multiple generated reports with the help of a token number, such as audit reports with different intervals. (g) Third-Party Integration: Provision to support integration with relevant third-party systems, such as payment gateway integrations, interactive voice response (IVR) Integrations, SMS Gateway Integrations, etc. (h) Bill payment and reconciliation feature: Provision for bill payment	
--	--	--

	and reconciliation (in case a DPO is running service in post-paid mode). (i) Generation of Reports: Provision to generate the following reports for operational purpose: 1) All, selective and single boxes' current status with their first-time activation date. 2) Total number of à-la-carte channels and bouquets and STB/unique consumer subscription expiring detail till given future date on the dashboard, according to the permission. 3) Today's fresh activation count, de-activation count, re-activation count, à-la-carte channels and bouquets addition/removal count on dashboard, according to the permission. 4) Total active and inactive subscriber's details with multiple criteria (network-wise, à la-carte channels and bouquets-wise, state-city wise and broadcaster-wise).	
29	It shall be mandatory for SMS to have backup servers and logs of all activities carried out in main server shall be concurrently copied into the backup servers, in an automated manner without any manual intervention.	• Auditor to check and validate the same during the conduct of audit. • All details of backup servers shall be captured and reported in the audit report.

	Provided that a log of all such instances shall be maintained along with date and time stamp, where the backup server has been used as the main server: Provided further that the main and backup server shall always be in sync with regard all data, such as subscription data, STB/unique consumer subscription UA/MAC ID details, entitlement level information, etc.	• Declaration to be submitted by DRM vendor regarding backup server deployment.
--	---	---

Table 2: DRM Requirements for conditional access by subscribers and encryption for IPTV services

S. No.	DRM Requirements for conditional access by subscribers and encryption	Audit Procedure & Remarks
1	DPO shall ensure that the current version of the DRM in use do not have any history of hacking. A written declaration from the DRM vendor shall be required to be furnished on an annual basis as compliance of this requirement.	• Auditor will take the DRM vendor declaration from DPO for compliance.
2	DRM shall ensure all logs are un-editable, stamped with date and time of all transactions (all activations, deactivation, channel authorization/assignment and un-authorization / de-assignments and change in MAC ID/STB/ unique consumer subscription). The DRM shall not allow altering or modification of any logs. There shall be no	• Auditor will take the DRM vendor declaration from DPO for compliance. • Auditor will check through DRM application access whether any facility is available for DPO to modify or alter the logs.

	facility for the distributor/users to purge logs.	
3	DRM deployed do not have facility to activate and deactivate a Set Top Box (STB) /unique consumer subscription directly from the Graphical User Interface (GUI) terminal of DRM. All activation and deactivation of STBs/unique consumer subscription shall be done with the commands of the SMS (provided that such feature may be available only for specific testing. The command or access for such feature may be available with the highest system administration password. In all such cases a separate log file of such commands has to be maintained) integrated with DRM. The DRM shall be integrated with the SMS in a manner that ensures security of the channel.	• Auditor will take the DRM vendor declaration from DPO for compliance. • Auditor will check through DRM application access whether such facility is available for DPO to activate and deactivate a Set Top Box (STB) /unique consumer subscription directly from the Graphical User Interface (GUI) terminal of DRM.
4	The SMS and the DRM should be integrated in such manner that activation and deactivation of STB/unique consumer subscription happen simultaneously in both the systems. Explanation: Necessary and sufficient methods shall be put in place so that each activation and deactivation of STBs/unique consumer subscriptions is reflected in the reports generated from the DRM.	• Auditor will check and validate the same by conducting simulation testing.
5	DRM deployed should be able to support two-way networks only.	• Auditor will take the DRM vendor declaration from DPO for compliance.

6	The DRM deployed should be able to support both carded as well as card-less STBs/unique consumer subscription for any provisioning.	• This may be checked by an auditor and recorded in report.
7	The DRM deployed should be able to generate, record, maintain independent reports and logs for verification purpose during audits corresponding to each command executed in the DRM issued by the SMS integrated with the DRM for last three (3) years minimum. The reports must have date and time stamp. Proposed reports should include: (a) Unique active STB/unique consumer subscription count as well as MAC ID wise on any desirable date. (b) Unique bouquet/channel active for a specific STB/unique consumer subscription on any desirable date I MACID/User ID wise activation-deactivation report for service requests (d) Any alteration in bouquet and/or channels configured in DRM I Blacklist STB/unique consumer subscription report (desirable not mandatory feature) (f) Product code pertaining to channels/ bouquets available on the platform (g) Channel/bouquet authorization/assignment to STB/unique consumer subscription along with start date and end date of entitlement	• Auditor to check and validate the availability of these reports/logs in the DRM deployed by the DPO during the audit. • Sample screenshots or sample logs may be enclosed with the audit report.

(h) STB/unique consumer subscription -VC pairing / de-pairing or User id- Mac-id Pairing / de-pairing (if applicable) in SMS/DRM (i) STB/unique consumer subscription activation/ de-activation (j) Channels assignment to STB/unique consumer subscription (k) Report of the activations or the deactivations of a particular channel for a given period (l) The total number of registered subscribers (m) The total number of active subscribers (n) The total number of temporary suspended subscribers (o) The total number of deactivated subscribers (p) List of blacklisted STBs/unique consumer subscription in the DRM (desirable not mandatory feature) (q) Channel and bouquet wise monthly subscription report in the prescribed format. I The names of the channels forming part of each bouquet (s) The total number of active subscribers subscribing to a particular channel or bouquet at a given time (t) The name of a-la carte channel and bouquet subscribed by a subscriber (u) The ageing report for subscription of a particular channel or bouquet.	
---	--

8	DRM deployed should be able to tag and blacklist the STB/unique consumer subscription in case of any piracy	• Auditor to validate the blacklisting capability of DRM during simulation testing. • Screenshots may be attached with the audit report. • (Note: If the hardware STB is not deployed and the user is doing piracy through software application then the linked Unique Consumer subscription mapped with Registered Mobile Number (RMN) and/or email needs to be blacklisted by the DRM.)
9	DRM deployed should have the technical capability in India to maintain the systems on 24x7 basis throughout the year	• Declaration from DRM vendor to be provided by the DPO.
10	The DRM and SMS should be integrated in such manner that upon deactivation of any subscriber from the SMS, all program/services shall be denied to that subscriber.	• Auditor to verify the same by conducting simulation testing and record in Audit report.
11	The DRM should be capable of generating, recording and preserving unedited data / logs for at least three consecutive years for each command executed through the DRM, including logs of each command of the SMS integrated with the DRM.	• Auditor to check and validate the availability of these reports/logs in the DRM deployed by the DPO during the audit. • Sample screenshots or sample logs may be enclosed with the audit report.
12	DRM deployed should be capable to support both software base as well as hardware base security.	• Declaration from DRM vendor to be provided by the DPO.
13	DRM shall be capable of adding/modifying channels/bouquets as may be required on real time basis in line with the activity performed in SMS.	• Auditor to check and validate the capability of the DRM during simulation testing. • Sample screenshots or sample logs may be enclosed with the audit report.

14	DRM should be so configured for specific type of STB/unique consumer subscription, that are procured and configured by the DPO. The DRM should not enable working/operation of any other type/brand/make of STB/unique consumer subscription, in the network.	• Declaration from DRM vendor to be provided by the DPO.
15	When infrastructure sharing (as and when permitted by MIB) is available, in such cases DRM shall be capable to support multiple DPOs.	• Declaration from DRM vendor to be provided by the DPO.
16	DRM should support content protection.	• Auditor to check and validate the same during simulation testing; and record in Audit report.
17	DRM should support key rotation, i.e., periodic changing of security keys	• Declaration from DRM vendor to be provided by the DPO.
18	In case DPO has deployed hybrid STBs (hybrid STB for the purpose of this regulation means a STB that uses multiple methods of receiving transmission signals with video and audio content, however in a single instance such STB provides only one type of service), DRM shall ensure that the over the-top (OTT) App and any browser does not get access to the linear television channels offered by the DPO from its own system, and similarly, DRM for IPTV service should not get access to channels delivered through OTT platform. Provided that, all the mandatory requirements for DRM shall be complied by hybrid STBs.	• Auditor to check and validate the same during simulation testing. • Declaration from DRM vendor to be provided by the DPO.

19	There shall not be any active unique subscriber outside the database tables. Further, there shall not be an option to split DRM database for creation of more than one instance by a DPO or a vendor.	• Auditor to obtain DRM Vendor Declaration regarding the no. of instances provided to DPO. • Auditor to check that no active subscriber is maintained outside the databases tables. • The DPO/DRM vendor will provide the necessary assistance and support to auditors for verification of compliance.
20	It must support the following options with reference to uploading of unique access (UA)/MAC ID details in DRM database: (a) A secure un-editable file of MAC ID details, as purchased by the distributor, to be uploaded by the DRM vendor on the DRM server directly, (b) If it is uploaded in any other form, UA/MAC ID in DRM database shall be captured in logs, I Further, DRM shall support an automated, application programming interface (API)-based mechanism to populate such UA/MAC ID details in the SMS, without any manual intervention.	• Auditor to check and validate the same during audit conduct; and record in Audit report.
21	It shall be mandatory to have backup servers and logs of all activities carried out in main server shall be concurrently copied into the backup servers: Provided that a log of all such instances shall be maintained along with date and time stamp, where the backup server has been used as the main server:	• Auditor to check and validate the same during the conduct of audit. • All details of backup servers shall be captured and reported in the audit report. • Declaration to be submitted by DRM vendor regarding backup server deployment.

	Provided further that the main and backup server shall always be in sync with regard all data, such as subscription data, STB/unique consumer subscription UA/MAC ID details, entitlement level information, etc.	
22	DRM and SMS shall ensure that the access to database is available to authorized users only, and in “read only” mode only. Further, the database audit trail shall be permanently enabled. Explanation: Database here refers to the database where data and log of all activities related to STB/unique consumer subscription activation, deactivation, subscription data, STB/unique consumer subscription UA/MAC ID details, entitlement level information, etc., is being stored.	• DRM vendor will provide declaration for database security and its restricted access to authorized users.
23	Provision of à-la-carte channels or bouquet: (a) DRM (and SMS) shall be able to handle all the channels, made available on a platform, in à la carte mode. (b) DRM (and SMS) shall have the capability to handle such number of broadcasters /DPO bouquets, as required by the DPO.	• Auditor will check and validate the same during simulation testing; and record in Audit report.
24	DRM and SMS applications, along with their respective databases, shall be stored in	• Auditor will check and validate the same during conduct of audit; and record in Audit report.

	such a way that they can be separately identified.	
25	DRM shall have a provision to export the database/report for reconciliation with the SMS database. Further, there shall be a provision of reconciliation through secure APIs/secure scripts.	• Auditor will check and validate the same during conduct of audit; and record in Audit report.
26	There shall be unique license key required for viewing, the encryption period for a specific key should be configurable to change at periodic interval in DRM deployed by DPO.	• Auditor to check and validate the same during audit; and record in Audit report.
27	For every change in channels, fresh license keys should be issued by the DRM. License keys issued by DRM should be secure and encrypted. DRM must ensure that the authorization keys are not received by the STB/unique consumer subscription from any other source other than the one specified by the IPTV system.	• The DPO to provide DRM Vendor Declaration to the auditor for compliance.
28	DRM servers should comply with extant Rules and Regulations including relevant clause under extant provisions (if any) relating to data localization, data security and privacy. It should not be allowed to connect main DRM server to some other location (India or other country) with some proxy or another server to integrate with SMS and DPO system.	• The DPO to provide DRM Vendor Declaration to the auditor for compliance.
29	IPTV service delivery may conform to multicast and/or unicast mode. The system configuration should ensure that	• The DPO to provide DRM Vendor Declaration to the auditor for compliance.

	every television channel is available to every customer on selection to view, irrespective of the mode of delivery or the number of viewers seeking such channel at any point of time. STBs/unique consumer subscription with facilities for recording programs shall have a copy protection system (i.e., a feature which prevents reproduction of content and/or unauthorized copying and distribution of content) and such recorded content should not be transferrable to any other device or delivered to any other network in any manner whatsoever.	• Auditor to check and validate the multicast/unicast delivery of content while conducting the audit. • Auditor to check and confirm whether the DRM deployed have copy protection mechanism enabled.
30	IPTV system should not be allowed to deliver linear content to any other device except STB/unique consumer subscription which has been whitelisted in DRM.	• Auditor to check and confirm during simulation testing that linear content delivery is not allowed to any other device.
31	The DRM should have following features: (a) It should restrict user to editing. (b) It should restrict user from sharing or forwarding or mirroring the content from the STB/unique consumer subscription. (c) It should disallow user to take screen shots or screen grabs or screen-recording, if technically feasible. (d) It should lock access to authorized STBs/unique consumer subscriptions only. (e) It should have Geo	• The DPO to provide DRM Vendor Declaration to the auditor for compliance. • Auditor to check the same during simulation testing and record observations.

	blocking feature. (f) It should be able to set expiry date to recorded content at STB/unique consumer subscription end based on various policies.	
32	The DRM should have the capability of being upgraded over-the-air (OTA) so that the connected STBs/unique consumer subscription always have the most upgraded version of the DRM.	• The DPO to provide DRM Vendor Declaration to the auditor for compliance.
33	The DPO shall ensure that the DRM is up to date by installing necessary patches, error corrections, additions, version releases, etc. so as to ensure protection of channels and content at all times.	• The DPO to provide DRM Vendor Declaration to the auditor for compliance.
34	No such functionality should be added to or removed from the DRM which compromises security of channels. DPO shall be responsible for encryption of channels' signals before their delivery through its IPTV platform using DRM hybrid STBs/unique consumer subscription. All costs / expenses (by whatever name called) that are required to be incurred or become payable for such upgradation and for delivery/distribution of multi-channel television programmes to subscribers shall be borne solely by such DPO. The DPO shall employ all reasonable security systems and procedures to prevent any loss, theft, piracy,	• Auditor to check and validate the same during audit.

	un-authorized use, reception or copying of channels or any part thereof and shall notify broadcasters as soon as practicable after it becomes aware that such an event has occurred.	
35	The DRM should not in any way interfere with / invalidate fingerprinting.	• Auditor to check and validate the same during simulation testing; and record in Audit report.
36	DPO shall promptly, and at its sole cost and expense, correct any issues with the DRM (such as bugs, defects, omissions or the like) that prevents subscribers from accessing the DRM hybrid STBs/unique consumer subscription or channels through the DRM hybrid STBs/unique consumer subscription.	• The DPO will provide Declaration to the auditor for compliance on its letter head.
37	DPO shall provide broadcasters with video and audio codecs supported by the DRM hybrid STBs/unique consumer subscription. The DPO shall ensure that no such changes/modifications are made to such codecs parameters that will require broadcasters to incur any expense for delivery of channels / content that are free from viewer discernible problems (including, without limitation, video with no audio, audio with no video or significant signal distortion).	• The DPO will provide Declaration to the auditor for compliance on its letter head.
38	DRM should ensure that the hybrid STBs/unique consumer subscription are verifiably	• Auditor to check and validate the same during the conduct of audit.

	located within India by reference to internet protocol address and service address. DRM must ensure and lock the viewership to single device by single STB/unique consumer subscription or any device by ensuring MAC ID based authentication. The DRM must use industry-standard means (including IP-address look-up technology with screening and blocking of proxies (including anonymizing and spoofed proxies)) to prevent delivery of channels to IP addresses outside of India or to proxies.	• Declaration to be submitted by DRM vendor regarding the compliance.
39	DRM should ensure that television channels are accessible on STBs/unique consumer subscription of only such subscribers who are then-current, valid subscribers of the DPO, and such confirmation must take place prior to the DRM delivering (or authorizing the delivery of) television channel to the STBs/unique consumer subscription of such subscribers.	• Auditor to check and validate the same during audit.
40	Upon deactivation of any subscriber from the SMS, the DRM shall restrict delivery of all programme/services to that subscriber.	• Auditor to check and validate the same during audit conduct.
41	The DRM should not have any feature to insert any content (including advertisement, banner on portion of screen, etc) by itself. However, ticker messages for consumer information as regards	• Auditor to check and validate during simulation testing; and record in Audit report.

	their services from DPO shall be permitted.	
42	The DRM should not mask/remove any copyright, trademark or any other proprietary information on the channels at the time of their delivery.	• Auditor to check and validate during simulation testing; and record in Audit report.

TABLE 3 : FINGERPRINTING REQUIREMENT UNDER DRM:

S. No.	Fingerprinting requirements under DRM	Audit Procedure & Remarks
1	The DPO shall ensure that it has systems, processes and controls in place to run fingerprinting at regular intervals.	• Auditor to check and validate during simulation testing.
2	The STB/Unique Consumer subscription should support both visible and covert types of finger printing.	• Auditor to check and validate the same during the simulation testing. • Supporting screenshots may be enclosed with the audit report.
3	The fingerprinting should not get invalidated by use of any device or software.	• Auditor to check and validate the same during the simulation testing.
4	The fingerprinting should not be removable by pressing any key on the remote of STB/ Unique Consumer subscription.	• Auditor to check and validate the same during the simulation testing.
5	The finger printing should be on the topmost layer of the video.	• Auditor to check and validate the same during the simulation testing.
6	The finger printing should be such that it can identify the unique STB/unique consumer subscription number or the unique VC number or the MAC ID.	• Auditor to check and validate the same during the simulation testing. • Supporting screenshots may be enclosed with the audit report.

7	The finger printing should appear on the screens in all scenarios, such as menu, Electronic Programme Guide (EPG), settings, blank screen, and games etc.	• Auditor to check and validate the same during the simulation testing. • Supporting screenshots may be enclosed with the audit report.
8	The location, font colour and background colour of fingerprint should be changeable from head end and should be random on the viewing device.	• Auditor to check and validate the same during the simulation testing.
9	The finger printing should be able to give the numbers of characters as to identify the unique STB/unique consumer subscription and/or the MAC ID.	• Auditor to check and validate during simulation testing.
10	The finger printing should be possible on global as well as on the individual STB/ Unique Consumer subscription.	• Auditor to check and validate the same during the simulation testing.
11	The overt fingerprinting/watermarking should be displayed by the DPO without any alteration with regard to the time, location, duration and frequency.	• Auditor to check and validate the same during the simulation testing.
12	The DRM deployed should be able to generate fingerprinting/watermarking both global fingerprinting as well as targeted channel fingerprinting/watermarking.	• Auditor to check and validate the same during the simulation testing. • Sample screenshots may be enclosed with the audit report.
13	The DRM shall support and enable forensic watermarking at STB/ Unique Consumer subscription level.	• Auditor to check and validate the same during the simulation testing. • Sample screenshots may be enclosed with the audit report.
14	The DRM shall have the capability to run fingerprinting with at least one fingerprinting every ten (10) minutes on a	• Auditor to check and validate the same during the simulation testing.

	24x7x365 basis. DRM should have a feature to publish report of fingerprinting schedule for defined interval. The DPO shall make such report available to broadcaster on request.	
--	--	--

TABLE 4: STB/ UNIQUE CONSUMER SUBSCRIPTION REQUIREMENTS UNDER DRM:

S. No.	STB/unique consumer subscription Requirements	Audit Procedure & Remarks
1	All STBs/unique consumer subscription should have a DRM content protection.	• Auditor to check and validate the same during the simulation testing.
2	The STB/unique consumer subscription deployed should be capable to support content decryption, decoding and DRM license evaluation.	• STB/unique consumer subscription vendor declaration to be submitted by DPO.
3	The STB/ Unique Consumer subscription should be capable of displaying fingerprinting inserted from Headend through DRM/SMS. The STB/ Unique Consumer subscription should support both targeted channel fingerprinting as well as all global fingerprinting.	• Auditor to check and validate the same during the simulation testing. • Sample screenshots may be enclosed with the audit report.
4	The STB/ Unique Consumer subscription should be individually addressable from the Head-end.	• Auditor to check and validate the same during the simulation testing.
5	The STB/ Unique Consumer subscription should be able to receive messages from the Head-end.	• Auditor to check and validate the same during the simulation testing.

6	The messaging character length should be minimal of up to 120 characters.	• Auditor to check and validate the same during the simulation testing.
7	There should be provision for global messaging, group messaging and the individual STB/ Unique Consumer subscription messaging.	• Auditor to check and validate the same during the simulation testing.
8	The STB/ Unique Consumer subscription must be compliant to the applicable Bureau of Indian Standards.	• Auditor to check and validate the same during the simulation testing. • For Software application based IPTV system, certificate from application developer/vendor shall be submitted. (BIS is Applicable for IPTV systems with Hardware/STBs. For Software application based IPTV system, certificate from application developer/vendor may be submitted for compliance.) Note: Software Application vendor is also required to submit security audit testing certificate from CERT-IN empanelled agencies along with declaration certificate.
9	The STBs/ Unique Consumer subscription should be addressable over the air to facilitate OTA software upgrade.	• STB Vendor/Application provide with provide declaration.
10	The STBs/ Unique Consumer subscription with facilities for recording the programs shall have international standard copy protection system.	• Auditor to check and validate the same during the simulation testing. • If the recording facility is available the recorded content shall only be played on the authorized device/user. It

		cannot be retransmitted outside to any user, nor can the recorded content be played if the customer is deactivated/suspended by the DPO.
11	The STB/ Unique Consumer subscription should have a provision that fingerprinting is never disabled.	• Auditor to check and validate the same during the simulation testing.
12	The watermarking network logo for all pay channels shall be inserted at encoder end only.	• Auditor to check and validate the same during the simulation testing. • Sample screenshots may be enclosed. • Applicable for encoder deployed in IPTV Headend after 2023.
13	DRM/SMS deployed should be able to send scroll messaging which should be only available in the lower part of the screen.	• Auditor to check and validate the same during the simulation testing. • Sample screenshots may be enclosed
14	DRM deployed should be able to geo tag STB/ Unique Consumer subscription deployed in the network for security.	• Auditor to check and confirm whether the IP of the STB/Unique subscription is captured in the DRM. The IP capture than should be tracked for identifying the locations of the STB/Unique Consumer Subscription. • Screenshots may be annexed with the audit report.
15	STB/ Unique Consumer subscription should take all commands directly from DRM not from any intermediate servers.	• Auditor to check and validate the same during the simulation testing.

16	STB/unique consumer subscription while using IPTV infrastructure should not have feature to download (direct or side download) any 3rd party App/APK and should not have access to any browser.	• Auditor to check and validate the same during the simulation testing. • STB/unique consumer subscription vendors will provide declaration on its letterhead for compliance
17	STB/ Unique Consumer subscription should not be able to access the authorization keys from any other source except from the IPTV system through the IPTV closed network. DRM must ensure that the authorization keys are not received by the STB/ Unique Consumer subscription from any other source other than the one specified by the IPTV system	• DPO are required to submit DRM vendor Declaration to the auditor. • Auditor to check and validate the same during the simulation testing. • Auditor may connect IPTV application/STB/User on some other Wi-Fi/mobile hotspot and check whether the IPTV services are still accessible.
18	No play store should be accessible for enabling download, etc. when STB/unique consumer subscription, is functioning in the IPTV network.	• Auditor to check and validate the same during the simulation testing. • STB/unique consumer subscription vendors will provide declaration on its letterhead for compliance.
19	STB/unique consumer subscription should have copy protection.	• Auditor to check and validate the same during the simulation testing.
20	DPO system should have capability to maintain un-editable logs of all activity and configurations including download or upgrade of IPTV services App (if any) at STB/unique consumer subscription end.	• Auditor to check and validate the same during the simulation testing. • STB/unique consumer subscription vendors will

		provide declaration on its letterhead for compliance
21	The DRM should not allow delivering linear TV channels on Internet. The delivery of multi-channel television programmes should remain in a closed network within the device.	• Auditor to check and validate the same during the simulation testing.
22	The STB/ Unique Consumer subscription should have forced messaging capability including forced finger printing display.	• Auditor to check and validate the same during the simulation testing.
23	The DRM hybrid STBs/unique consumer subscription should be tested for the following prior to their seeding in the subscribers' premises: (a) System down testing (b) Error messaging (c) Negative user journey testing (d) Device variance testing (e) Destructive testing (f) Application monitoring testing (g) In-app monitoring testing	• STB/unique consumer subscription vendors will provide declaration on its letterhead for compliance

8. Timelines under pre-signal/Compliance Audit

8.1 Every audit should be completed within four weeks for one Headend (Headend with one SMS and two DRM architecture). For DPO, with multiple headends and additional DRM/SMS systems, the suggested time for completing the audit is eight weeks. The time suggested is inclusive of audit visits, data analysis and issuance of audit report. These timelines have been given for the benefit of DPO as well as auditors so that the final audit reports are submitted by due date as prescribed in the Interconnection Regulations 2017.

8.2 In case verification and analysis of ground VC/Unique Consumer Subscription is also required, then the auditor may take additional one week for sample verification of the recordings and ground VC/Unique Consumer Subscription. Provided that in case of broadcaster caused audit, the auditor may take additional time (depending upon the location and no of samples to be tested) as mutually agreed between the Broadcaster, DPO and Auditor.

8.3 In case the broadcaster has any issues/doubt/clarifications with the audit report shared by the DPO the same needs to be communicated by broadcaster within forty-five days⁷ after the receipt of audit report.

9. Subscription Audit

9.1 Regulation 15 of the Interconnection Regulations 2017 specifies that every distributor of television channels shall get addressable system of its distribution platform, such as subscriber management system, conditional access system, digital rights management system, and other related systems audited once every year, for the preceding financial year, by an auditor, to verify the information contained in the monthly subscription reports made available by the distributor to the broadcasters, and the distributor shall ensure that the relevant audit report, including all annexures, is shared with each broadcaster with whom it has entered into an interconnection agreement, by the 30th September every year. It may be noted that all the subscription report for each month with respect to each broadcaster with whom the distributor has signed an agreement will be necessarily required to be checked by the auditor. This audit is generally called subscription audit. The audit fee for such audit will be borne by the distributor. As per sub-regulation (1) of Regulation 15, the annual Audit caused by distributor using DRM systems shall include the Audit to validate compliance with the Schedule X of the Interconnection Regulations 2017

⁷ As per Seventh Amendment Regulations 2026.

and the Subscription Audit, as provided for in the Interconnection Regulations 2017.

In case of new distributor, before acquiring the content, no such subscription reports would be available for verification. The auditor will duly record this fact and carry the audit on all other aspects.

- 9.2 The subscription audit's focus is on ascertaining the subscriber numbers being reported by distributors to broadcaster. As per the Interconnection Regulation 2017 any variation, due to audit, resulting in less than zero point five percent of the billed amount shall not require any revision of the invoices already issued and paid.
- 9.3 Therefore, in addition to compliance audit, DPOs are required to conduct the subscription audit every year and share the copy of the report with every broadcaster with whom interconnection agreements are signed.
- 9.4 Sub-regulation (2) of Regulation 15 of the Interconnection Regulations 2017 also permits a broadcaster to cause audit of DPO subject to certain conditions specified in the Interconnection Regulations 2017 (as amended).
- 9.5 The audit fee for compliance audit or subscription audit commissioned by a broadcaster to re-verify the addressable system requirements, will be payable by the broadcaster.
- 9.6 In case the audit conducted under sub-regulation (1) or sub-regulation (2) or sub-regulation (2A) of Regulation 15 of the Interconnection Regulations 2017 reveals that –
- a) there is a discrepancy in the number of subscribers, the payment amount may be settled in accordance with the provisions of the interconnection agreement entered between the broadcaster and the distributor;

- b) the addressable system being used by the distributor does not meet the requirements specified in the Schedule III or the Schedule X or both, it shall be permissible to the broadcaster to disconnect signals of television channels, after giving written notice of three weeks to the distributor.

9.7 It may be noted that the scope of subscription audit will be limited to validation of the monthly subscriber report submitted by DPO to the respective broadcaster with whom interconnection agreements are signed.

10.Scope of work under Subscription Audit

10.1 In view of the section 15 of the Interconnection Regulations 2017, the scope of subscription audit will be limited to validation of the monthly subscriber report submitted by DPO to every broadcaster with whom interconnection agreements are signed. However, in order to ensure the sanctity of data certain checks regarding integration of SMS and DRM will also be carried out by the auditor before data extraction.

10.2 All headends should be visited and covered in the audit while conducting the subscription audit.

10.3 Auditor will verify the integration of the DRM and SMS deployed by DPO by performing few simulation tests on sample STBs such as activation/deactivation, fingerprinting and messaging command and generating respective reports from both SMS and DRM. The auditors will then check the SMS and DRM logs also regarding command execution timings to validate the integration between DRM and SMS.

10.4 After verification of integration of DRM and SMS deployed by DPO (or after conducting compliance audit), auditor needs to carry out data extraction from the SMS and DRM as per the scope mentioned below.

- i. *Extraction of as on date data dumps from the SMS and DRM server deployed by DPO for SMS and DRM data reconciliation.*
- ii. *Analysis on the data dump to verify the 20% random sample weeks of the audit period in respect of monthly subscriber report submitted by DPO to every broadcaster. The auditor is required to verify the MSR data for every pay channel of broadcasters available on DPO's network for these 20% sample weeks selected on random basis by the auditor covering at least one week of every month for the entire audit period.*

Note: If variance of more than 1% is noted by the auditor in the MSR report of a-la-carte/package of any broadcaster in the 20% random sample weeks selected by the auditor, then auditor is required to validate the MSR Report of that particular broadcaster for the entire audit period of that a-la-carte channel/package.
- iii. *Analysis on data dumps to verify the as on date active⁸count of STBs/Unique Consumer Subscription available on the IPTV system of the DPO.*
- iv. *Analysis on data dump to report the active STB/ Unique Consumer Subscription count on 5 random dates from the audit period other than 7th, 14th, 21st and 28th.*
- v. *Verification of as on date DPO package wise, a-la-carte and broadcaster bouquet wise STB/VC/Unique Consumer Subscription details (both from SMS & DRM system). In case of variance of more than 15% of the "as on date" data and the audit period data, the auditor shall bring the variance to the notice of concerned broadcaster.*
- vi. *Verification and reporting of Channel to package mapping along with service ID (with creation, modification and discontinue date) from SMS*

⁸ As the intent of audit is to verify subscribers numbers, the audit may be limited to active STBs only. Any reconciliation or audit needs to be carried on the active count of SMS and DRM.

& DRM on the minimum 20% random selected dates of the audit period (as per point ii above).

vii. Reconciliation of complete VC/STB/unique consumer subscription data from DRM and SMS as on date of audit. Any discrepancy of VC/STB/Unique Consumer Subscription not active in SMS but found active in DRM, excluding test/monitoring VC/STB/Unique Consumer Subscription, or vice versa should be reported in actual numbers as well as percentage of the total base.

10.5 Details of test/monitoring VC/STB/Unique Consumer Subscription should be separately recorded.

10.6 Auditor will ensure that no parallel SMS or DRM systems which are not reported by DPO are deployed in the headend of DPO where the audit is being carried out by auditor.

10.7 Reconciliation of DPO's LCN and Genre with the actual LCN and genre found during audit field visit. All mismatches of LCN and genres found during audit to be reported.

10.8 The Auditor shall connect/activate the Set-Top Box (STB)/ Unique Consumer Subscription to the Distribution Platform Operator (DPO) signal at the Headend, scroll through the complete channel lineup, and prepare a consolidated record of each channel's LCN, name, and genre as displayed on the EPG against the actual broadcast content observed on screen. All discrepancies in LCN allocation, channel naming, or genre classification shall be documented, and a report of mismatches with corrected LCNs and genres shall be reported.

10.9 Analysis and verification of VC samples (STB/Unique Consumer Subscription) provided by broadcasters may also need to be covered under scope of work. However, the procedure to be followed for carrying out such

analysis and verification are mentioned separately in the section 17 of the audit manual.

10.10 The above scope of work will also be applicable in case of infrastructure sharing (if applicable) between multiple DPOs.

- In the course of auditing an infrastructure seeker, the scope of review shall be limited to the seeker's DAS and the elements obtained through infrastructure sharing arrangements from the infrastructure provider⁹.
- When auditing an infrastructure provider, the audit shall encompass all DAS elements under its ownership and the elements shared with the infrastructure seeker through infrastructure sharing arrangements.

For ease of doing business and audit it would be advisable for infrastructure providers and seekers to conduct audit of their DAS system jointly (provider + seeker) especially when they are sharing DRM/SMS or both.

In the case of sharing of DRM/SMS or both, broadcaster(s) can conduct joint and simultaneous audits covering all elements of all the DPOs sharing the infrastructure, as per the Interconnection Regulations 2017 (as amended), if required.

11. Documents required under Subscription audit by auditor

11.1 Valid DAS license/permission issued by Ministry of Information and Broadcasting.

⁹ Audit may be restricted to infrastructure sharing seeker and related elements of the infrastructure sharing provider. Justification for the same is that the other elements under audit of infrastructure sharing provider such as DRMSMS, mux, encoders, etc. which are not related to Infrastructure sharing seeker will unnecessary result in additional time and resources of the stakeholders that are involved in this process without any material effect on the audit.

- 11.2 Block schematic diagram of Headend including DRM and SMS.
- 11.3 Certificate from all the DRM vendors **(Format as in Annexure 1).**
- 11.4 Certificate from SMS vendors **(Format as in Annexure 2).**
- 11.5 Certificate from STB Vendor (If applicable) **(Format as in Annexure 4).**
- 11.6 Certificate from Software Application Vendor in user device **(Format as in Annexure 5).**
- 11.7 Signed and stamped copy of subscription audit form as per **Annexure 6.**
- 11.8 Signed and stamped copy from Infrastructure Provider (If applicable) as per **Annexure 9.**
- 11.9 **Monthly SMS report regarding state wise active¹⁰ STB count for the audit period. This report is applicable for all DPOs who have operations in different states.**
- 11.10 It may be noted that in case system generated reports capture all the fields specified in the above declaration format, then the auditor may accept such system generated reports.¹¹

12. Methodology to be adopted for Subscription audit

- 12.1 The audit either will be caused by the DPO or Broadcaster by selecting any of the audit agencies empanelled by TRAI or BECIL.

¹⁰ As the intent of audit is to verify subscribers numbers, the audit may be limited to active STBs only. Any reconciliation or audit needs to be carried on the active count of SMS and DRM.

¹¹ It has been brought to the notice of TRAI that sometimes auditors insist on certain specific formats which suit their reporting requirements. This creates problem for DPOs whose audits are conducted by different auditors to provide such specific reports. This amendment will help to address this issue.

- 12.2 Once the audit is scheduled, the auditor will immediately ask DPO whether he has any objections regarding usage of his/her laptop for the conduct of audit.
- 12.3 If DPO wants to provide its own laptop for conduct of audit then auditor needs to convey its requirement of software or any other tools required during the conduct of audit.
- 12.4 The DPO shall respond immediately on the same whether he is willing to provide laptop and other necessary tools/software required or wants auditor to use his/her own laptop.
- 12.5 The minimum configuration requirement of laptop is mentioned in section 19 of the Audit Manual which should be provided by DPO to auditor. DPO is free to provide laptop of higher configuration also.
- 12.6 The DPO should inform all the broadcaster with whom it has entered into an interconnection agreement, at least thirty days in advance, the schedule of audit and the name of the auditor, in case of DPO caused audit. In case of broadcaster caused audit, broadcaster shall inform concerned DPO about the name of the auditor and schedule audit in consultation with DPO. Such audit must commence within 30 days of notice.
- 12.7 The auditor will also share the document requirements with DPO as specified in Section 11 of the Audit Manual before the conduct of audit.
- 12.8 **Auditor will cover all the scope of work mentioned in section 10 of the audit manual during subscription audit.**
- 12.9 The data extraction procedure from DRM and SMS should be carried out as mentioned in section 16 of the Audit Manual.

- 12.10 In case of DPO having multiple head ends, the auditor is required to visit each and every headend and ensure all audit checks as mandated by TRAI Regulations are conducted.
- 12.11 After completion of subscription audit, auditor shall ensure that subscription report w.r.t. a particular broadcaster contains information in respect of his channels and bouquets only. For example, if there are 20 broadcasters with whom interconnection agreements are signed then 20 such broadcaster wise subscription reports are required to be made complete with all annexures.
- 12.12 If the audit is caused by the broadcaster, then the auditor will share the audit copies both with the broadcaster as well as the DPO.

13. Procedure to be followed for inspection of Subscription audit

- 13.1 The primary objective of the subscription audit is to validate the monthly subscriber report submitted by DPO to its respective broadcasters.
- 13.2 In this regard, scope of work to be covered and data extraction methodology to be adopted under subscription audit is specified in section 10 and section 16 of the Audit Manual.
- 13.3 Thus, auditor needs to ensure that the subscription audit should be carried out keeping in view the scope of work and data extraction procedure mentioned in the Audit Manual.
- 13.4 The format of the report required under subscription audit is provided in the **Annexure 7** of the audit manual.

- 13.5 No specific analysis procedure on data dump is specified here, and the auditor is free to choose his/her own analysis method, tools, software to achieve the desired results.

14. Scheduling of Subscription Audits

- a) All the DPOs are required to conduct the subscription audit within a year as mandated by the Interconnection Regulations 2017 (as amended). Every distributor of television channels shall get addressable system of its distribution platform, audited once every year, for the preceding financial year, by an auditor, to verify the information contained in the monthly subscription reports made available by the distributor to the broadcasters. The distributor shall ensure that the relevant audit report, including all annexures, is shared with each broadcaster with whom it has entered into an interconnection agreement, by the 30th September every year.

15. A. Timelines for completion of Subscription Audits

- a) The auditors are required to complete the subscription audit of DPO (one Headend, one SMS and two DRM) and submit the report within six weeks. For DPO, with multiple headends and additional DRM/SMS systems, the suggested time for completing the audit is 8 weeks. The time suggested is inclusive of audit visits, data analysis and issuance of audit report.
- b) In case where verification and analysis of ground VCs/Unique Consumer Subscription are also required the auditor may take additional one week for sample verification of the of ground VCs/Unique Consumer Subscription samples. Provided that in case of broadcaster caused audit, the auditor may take additional time (depending upon the location and no of samples to be tested) as mutually agreed between the Broadcaster, DPO and Auditor.

- c) In case the broadcaster has any issues/doubt/clarifications with the audit report shared by the DPO the same needs to be communicated by broadcaster within forty-five days¹² after the receipt of audit report.

B. Timelines for completion of both Technical and Subscription Audits

The auditors are required to complete both technical and subscription audit of DPO (one Headend, one SMS and two DRM) and submission of report within eight weeks. For DPO, with multiple headends and additional DRM/SMS systems, the suggested time for completing the audit is 10 weeks. The time suggested is inclusive of audit visits, data analysis and issuance of audit report.

16. Data Extraction procedure to be followed by the auditor under compliance and subscription audit

- 16.1 DPO to declare all admin/super admin login access to DRM & SMS servers and depute a resource who has complete knowledge of the systems (DRM and SMS). The resource can be common or different for DRM and SMS systems depending on his/her expertise.
- 16.2 The DPO resource under supervision of auditor will access both the systems and extract data and run queries.
- 16.3 Auditors are not allowed to interfere with the live systems (DRM and SMS) of DPO without his/her permission and assistance.
- 16.4 If the data extraction from the live SMS and DRM systems are not possible due to any technical issue or is taking excess time in extraction, then the auditor is allowed to use latest automated or manually

¹² As per Seventh Amendment Regulations 2026.

downloaded data dump from the server after due verification of the query used for downloading the same.

- 16.5 If the auditor is satisfied with the procedure of downloaded data dump and finds that the dump is not compromised or altered, he/she may use the same for audit purpose.

16.6 Note: The exemption of data extraction from live servers is only applicable for DPO who are having more than 5 lakhs subscriber base and when there is practical difficulty in extracting the data dump from live servers. This will be decided by the auditor after understanding the systems of such DPOs and in case they find explanations reasonable.

- 16.7 The DPO is also requested to share the database table's fields and column structure along with other necessary information required by auditor to work on the data dump to extract the active STB/VC count from the data dump.

- 16.8 If required, all extracted data should be loaded on PC/Laptop provided for Audit.

- 16.9 All data from DRM and SMS server should be extracted in such a manner that no active STB/VC/Unique Consumer Subscription is left out from the database. The Auditors should acquaint themselves with the data extraction queries that are run on the live DRM & SMS servers.

- 16.10 Data extraction queries' scripts and explanation of terminology used must be preserved.

- 16.11 The auditor should understand what all filters (if any) are being applied to either exclude data of other DPOs or even exclude data of certain geographical areas that may have a bearing on the overall count of the subscriber numbers.

16.12 Auditor should be present in-person during the extraction of DRM & SMS data. Auditor to certify that the data extraction has been done under his/her supervision.

17. Analysis and Verification of VC/Unique Consumer Subscription

17.1 As mentioned earlier, if the audit is caused by the DPO whether compliance or subscription audit then the distributor shall inform the broadcaster with whom it has entered into an interconnection agreement, at least thirty days in advance, the schedule of audit and the name of the auditor¹³.

17.2 The broadcasters may provide the Ground VCs/Unique Consumer Subscription (if any) to auditors for verification and analysis of the VCs/Unique Consumer Subscription samples before the conduct of audit.

17.3 If the audit (whether compliance or subscription audits) is caused by broadcaster, then broadcaster can directly share the information regarding VCs/Unique Consumer Subscription (if any) with the audit agency.

17.4 The analysis and verification of TS recordings shall be carried out as per following procedure:

- The broadcaster cannot share more than 100 VC/Unique Consumer Subscription samples with auditor in case the audit is caused by DPO. In case the audit is caused by broadcaster there is no restriction on sample size of VCs/Unique Consumer Subscription. Broadcaster should ensure that these VCs/Unique Consumer Subscription samples are correct and should be provided with date, time and complete address/location details.

¹³ As per Seventh Amendment Regulations 2026.

- The auditor should verify these VCs/Unique Consumer Subscription samples during conduct of audit. In case he/she is not able to find some VCs/Unique Consumer Subscription samples in the DRM and SMS database of DPO then random physical verification of such VCs/Unique Consumer Subscription samples should be carried out by auditor in order to validate the shared VCs/Unique Consumer Subscription samples.
- In such cases where a certain amount of VCs/Unique Consumer Subscription samples provided by broadcasters are not found in the DRM and SMS database of DPO then auditor will select minimum five (5) number of VCs/Unique Consumer Subscription/devices samples from these VCs/Unique Consumer Subscription samples on random basis for carrying out physical verification to ensure the correctness of samples.
- The cost of carrying out minimum physical verification of these VCs/Unique Consumer Subscription samples which are not found in the DPO system shall be borne by the DPO if the audit is caused by DPO.
- Further, any physical inspection cost during audit caused by broadcaster shall be borne by broadcaster however 5 minimum VCs/Unique Consumer Subscription samples needs to be carried out by auditor to validate the VCs/Unique Consumer Subscription samples which are not found/matched in the system of DPO.
- It may be noted that it should be the responsibility of broadcaster to provide necessary assistance and support to auditor during physical verification of ground samples whenever validation of such VCs/Unique Consumer Subscription samples is required.

18. Responsibilities in respect of Compliance and Subscription Audit

A. Distribution Platform Operator

- 1) The DPO should abide by the provisions of the Interconnection Regulations 2017.
- 2) The DPO should ensure that their technical systems are always compliant with TRAI regulations at all times; and subscriber numbers reported to the broadcasters in the MSRs are correct and accurate. DPO shall cause the compliance audit and the subscription audit of its system every year as specified in the Interconnection Regulations 2017.
- 3) Every DPO shall ensure the availability of complete data in DRM and SMS for minimum 3years from the date of conduct of audit.
- 4) It is the responsibility of DPO having shared DRM and SMS systems with its JV companies to share the complete data from SMS and DRM including JV company's data with auditor during compliance or subscription audit whether caused by DPO or broadcaster. Thus, it would be advisable for such a DPO to conduct audit of its complete DAS system including JV companies.
- 5) The DPO shall timely inform the broadcasters whenever compliance or subscription audit is scheduled at least 30 days in advance, the schedule of audit and the name of the auditor.¹⁴

¹⁴ As per Seventh Amendment Regulations 2026.

- 6) The DPO will share the relevant part of the report, including all annexures¹⁵, of the compliance audit and subscription audit caused by DPO with concerned broadcaster.
- 7) If the subscription audit of a DPO reveals that there is more than zero point five percent variance in the monthly subscription report submitted by the DPO to any of the broadcasters, then it is the responsibility of the DPO to inform such broadcasters for revision of the invoices already issued and paid.
- 8) The DPO will provide full support and assistance to the auditor conducting its audits, whether caused by self or broadcaster.
- 9) If the DPO does not want auditor to use his laptop for audit purpose, then it is the responsibility of the DPO to provide laptop of required configuration as mentioned in the audit manual or higher to the auditor. The specification in respect of minimum configuration of laptop to be provided by DPO is mentioned in section 19 of the Audit Manual.
- 10) The DPO also needs to ask auditor about any other specific requirements in advance regarding the software or tools required for data analysis purpose before the commencement of audit.
- 11) These equipment/software/tools shall be made available to the auditor at his disposal for usage during the conduct of audit whether audit caused by self or broadcaster.
- 12) DPO should inform broadcaster if below mentioned changes are made in its DRM, SMS and other related systems within 7 days from the implementation date of these changes:

¹⁵ As per Seventh Amendment Regulations 2026.

- a. Addition/Deletion of SMS***
- b. Change in the SMS version w.r.t last audited SMS***
- c. Addition/Deletion of DRM***
- d. Change in the DRM version w.r.t last audited DRM***
- e. Deployment of new type of STBs by DPO which were not audited earlier.***
- f. In case any DPO opts for infrastructure sharing (either provider or seeker) or shifts from one DPO to another for infrastructure sharing.***

- 13) Subject to conformance to Regulation 11 of the Interconnection Regulations 2017, the distributor may extend territory of interconnection agreement by giving a written notice to the broadcaster providing at least 30 days to the broadcaster. In such cases, the distributor shall also inform the broadcaster formally after 7 days of actual extension of the territory.
- 14) DPO should provide access to DRM, SMS servers and related addressable system to the auditor and depute a resource/expert of deployed DRM and SMS systems who will perform data extraction under supervision of auditor.
- 15) Auditor can demand specific data, logs and reports and the DPO should extract the data in front of the auditor and provide the same. DPO should ensure that no STB/VC/Unique Consumer Subscription is left out from the database.
- 16) The broadcaster may depute one representative to attend the audit and share inputs of the broadcaster for verification during the audit process and the distributor shall permit such representative

to attend the audit.¹⁶ The DPO should also allow broadcaster's representative to be physically present during the conduct of audit.

- 17) In case DPO has provided its own laptop (in this audit manual 'laptop' includes 'computer/PC/laptop') to the auditor for an audit, then DPO shall preserve the entire data used by the auditor till at least one year after that audit.¹⁷ In case of any ongoing legal dispute concerning the audit, the entire data should be preserved until such legal dispute is over.
- 18) In case of infrastructure sharing, infrastructure provider shall provide information related to infrastructure seeker(s) and shared elements as per **Annexure-8**.

B. Responsibility of Broadcaster

- 1) The Broadcaster should abide by the provisions of the Interconnection Regulations 2017.
- 2) The broadcaster should ensure that the correct ground VC samples (if any) are provided to auditors before conduct of audit whether compliance or subscription audit.
- 3) The broadcaster should also provide full support to auditor and provide necessary information if required by auditor such as fingerprint schedule, assistance in physical verification of sample ground VCs/Unique Consumer Subscription samples etc.
- 4) During DPO caused audit, the presence of the representative of the broadcaster is for the limited purpose of sharing inputs, if any, for verification during the audit process, and does not entitle him to

¹⁶ As per Seventh Amendment Regulations 2026.

¹⁷ Focus should be on preserving the data by any appropriate means for at least one year and not necessarily preserving the data in that particular laptop. This will result in blocking of a hardware without any purpose.

direct or influence, in any manner, the conduct of the audit¹⁸. During the audit initiated by broadcaster, the representative of broadcaster will not interfere with the audit proceedings during the conduct of audit. If there are any relevant concerns or objections the same shall be shared before the conduct of audit.

- 5) If the audit is caused by the broadcaster, then the broadcaster is not allowed to send more than one representatives to observe the audit proceedings.

C. Responsibility of Auditor

- 1) The auditor should abide by the provisions of the Interconnection Regulations 2017 and the terms and conditions of the empanelment by TRAI.
- 2) The Auditors' main role and responsibility is to carry out the above-mentioned compliance and subscription audits in an objective, transparent and impartial manner as per provisions of the Interconnection Regulations 2017.
- 3) It is the responsibility of auditor to keep all the data extracted or information collected during audit confidential and produce only the relevant information in the audit report. The auditor may also ensure that the data pertaining to one broadcaster is not shown/revealed/shared to another broadcaster.
- 4) In case the ground VCs/Unique Consumer Subscription samples are provided by broadcasters then auditor should verify that these VC samples are available in the DRM and SMS database of DPO.
- 5) If the shared VCs/Unique Consumer Subscription samples are not found in the DRM and SMS system of DPO then auditor will also

¹⁸ As per Seventh Amendment Regulations 2026.

carry out the physical verification of minimum 5 VCs/Unique Consumer Subscription samples to check the authenticity of same. These 5 samples shall be selected on random basis from the list of samples which were not found in the system of DPO.

- 6) The audit period shall be as specified in the Interconnection Regulations 2017¹⁹.
- 7) The auditor will not carry any data dump outside the DPO premises without his consent. If DPO is not comfortable with the auditor taking data out of its premises for analysis, then the auditor shall perform all the data analysis, for either compliance or subscription audit, at DPO premises only.
- 8) In such cases, the auditor only will be allowed to carry the result of data analysis along with other necessary documents such as screenshot of queries run, DRM and SMS generated reports and audit related documents (audit forms, vendor declarations, annexures etc.). The auditor will also provide a copy of these documents to DPO.
- 9) The auditor should not engage in any arguments or dispute with DPO during conduct of audit. If there are any issues or non-cooperation from DPO during audit, the auditor shall inform the DPO in writing that the audit could not be conducted.
- 10) If auditor feels any justification or explanation is required from DPO on any issue observed during the conduct of compliance or subscription audit, he/she may provide the opportunity to DPO before the finalization of audit report. The justification or

¹⁹ As per Seventh Amendment Regulations 2026.

explanation of DPO shall also be incorporated in the audit report along with the issue observed by the auditor.

- 11) The auditor will not insist on any specific format of the reports generated from the SMS and DRM systems as mandated in Schedule X of the Interconnection Regulations 2017 or any other report to be generated under scope of work of audit manual. However, the report should be able to reflect and produce desirable information.
- 12) The auditor will make non editable soft copy and hard copy of the audit report both for compliance and subscription audit. Further, number of copies of subscription audit report caused by DPO depends upon the number of broadcasters with whom interconnection agreements are signed by DPO.
- 13) In case the DPO is non-compliant to any of the provisions of extant regulation(s) then it is the responsibility of auditor to clearly mention the same in its report especially in the executive summary of the report so that it is clearly communicated to broadcaster.
- 14) The Auditor shall comply with all the instructions, guidelines, directions, orders etc. issued by TRAI, from time to time, for the purpose of conducting the audit of the Digital Addressable Systems of the Service Providers and reporting thereof.
- 15) The Auditor shall not undertake audit of addressable system of any service provider for whom the Auditor is also the statutory auditor or internal auditor or concurrent auditor or where the Auditor is the consultant to the service provider.
- 16) The Auditor shall not undertake audit of the addressable system of any service provider consecutively for more than three years.

- 17) The Auditor shall submit the report to TRAI about the details of audits carried out by the Auditor, as per the format prescribed by TRAI from time to time.
- 18) TRAI reserves the right to review, dissolve the panel of Auditors, extend the validity of the panel, expand the panel and remove any Auditor from the panel for unsatisfactory performance, at any time.
- 19) TRAI may remove any Auditor from the panel of empanelled auditors, in case, it is established that the Auditor has performed two erroneous audits.
- 20) The Auditor shall continue to meet all the eligibility conditions specified in the Expression of Interest for Empanelment of Auditors to carry out audit of Digital Addressable Systems, throughout the period of empanelment. The Auditor must immediately inform TRAI in case the Auditor fails to meet any of the eligibility criteria specified, at any time during the period of empanelment so that TRAI may remove the Auditor from the list of empanelled auditors. In case the Auditor does not inform, and it comes to the notice of TRAI through any source at a later date, then TRAI may take suitable action including but not limited to blacklisting the auditor and forfeiting performance bank guarantee and issuing press release in this regard.
- 21) The Auditor shall adhere to the conditions contained in the Expression of Interest and shall follow the Audit Manual prescribed by TRAI.
- 22) The Auditor and their staff/audit personnel must carry out the tasks with the highest degree of professional integrity and technical competence. They must be free from all pressures and

inducements, particularly financial, which might influence their judgment or the results of any assessment, especially from persons or groups of persons with an interest in such results.

- 23) The Auditor must guarantee the impartiality of inspection staff/audit personnel. Their remuneration must not depend on the number of assessments carried out or on the results of such assessments.
- 24) The auditor conducting the audit of the addressable systems, shall furnish the audit report, along with an audit certificate, to the distributor confirming that the auditor is independent of the auditee and that the audit was conducted in accordance with the provisions of the regulations, in the format as may be specified by the TRAI from time to time.
- 25) In case of any misconduct or negligence by the auditor; TRAI is free to report the matter at any time to any Government agency or department/statutory body/ICAI/ ICWAI or any other concerned professional body.
- 26) The Auditor shall maintain confidentiality as mentioned in the EOI.
- 27) The Auditor shall maintain, at all times during its period of empanelment, necessary office set up and adequate personnel to ensure proper deployment and timely completion of the assignments.
- 28) The Auditor shall not sub-contract the audit work assigned to the Auditor to any outside firm or other persons.
- 29) In case any information/documents submitted by the Auditor, whether at the time of submission of proposal or thereafter, to TRAI

is found to be incorrect or false or misleading, the Auditor shall be removed from the panel immediately. In addition, the audit agency and the professionals will be liable for appropriate action in accordance with statutory guidelines or professional rules.

- 30) TRAI reserves the right to remove the Auditor from the panel in case it is found that any of the conditions laid down in the Expression of Interest have been contravened or the performance of the auditor is found to be unsatisfactory or any serious act of omission or commission is noticed in the Auditor's working. In such a case the Auditor will be blacklisted for empanelment with TRAI for a period of two years. If felt necessary, the matter may be reported to ICAI and/or RBI/IBA/ICSI/ICWAI/BCI or any other concerned professional body for necessary action.
- 31) TRAI may call the auditor for meetings/presentation for seeking/providing clarifications or for reviewing the progress of audit. The auditor shall attend such meetings/presentation at its own expenses.
- 32) The auditor shall indemnify and hold TRAI harmless against all claims, demands, disputes or judgment of any nature brought against TRAI arising out of the services provided by the auditor to the service provider under this agreement. TRAI shall be entitled to get the monetary loss suffered by it, if any, reimbursed from the auditor. TRAI may also, at its discretion, remove the auditor from the panel in such circumstances, without prejudice to the auditor's obligation under this clause, which shall survive the auditor's removal from the panel.
- 33) In case of disputes/clarifications arising out of EOI, the decision of TRAI shall be final and binding on the auditor.

- 34) The auditor shall comply with and be governed by the laws of India for the time being in force.
- 35) In case auditor has used its own laptop for an audit, then the Auditor shall preserve entire data²⁰ of the DPO till at least one year after that audit. This is in case DPO had no objection to auditor using its own laptop and DPO permits auditor to take data outside its premises. Besides, in such cases, DPO shall also preserve entire data given to auditor and/or extracted by auditor, till at least one year after that audit. In case of any ongoing legal dispute concerning the audit, the entire data should be preserved until such legal dispute is over.

19. Minimum Laptop Configuration to be provided by DPO

Particulars	Subscriber base > 50 Lakhs	Subscriber base between 10 Lakh to 50 Lakh	Subscriber base between 1 Lakh to 10 Lakh	Subscriber base less than 1 Lakh
Processor	Intel® Core™ i7	Intel® Core™ i5 or i7	Intel® Core™ i5 or i7	Intel® Core™ i5 or i7
Hard Disk Space available in C drive	1 TB or above	500 GB or above	500 GB or above	100 GB or above
RAM	16 GB or above	16 GB or above	8 GB or above	8 GB or above
Partition in drive	No partition required in the drive, need a single drive	No partition required in the drive, need a single drive	Not Applicable	Not Applicable
Data source location (Local/Server)	RDP	Local or RDP	Local	Local
Operating System – 32 bit / 64 bit	Windows 64bit	Windows 64bit	Windows 64bit	Windows 64bit
Microsoft SQL Server	Microsoft SQL Server	Microsoft SQL Server	Microsoft SQL Server	Microsoft SQL Server Express/

²⁰ The data extracted during an audit takes significant storage space in the laptop. Auditors usually use their own laptop for multiple audits. After analysis of the data, a copy of the entire data might be needed to be stored securely on some external storage device or Secure FTP or cloud storage and then deleted from the auditors laptop to free up storage space. Hence, the focus should be on preserving the data by any appropriate means for at least one year and not necessarily preserving the data in that particular laptop used by the auditor.

Management Studio & SQL Server Data Tools (SSDT)	developer edition	developer edition	developer edition/Microsoft Access	developer edition, Microsoft Access, Microsoft Excel
	(not Express edition)	(not Express edition)	(not Express edition)	Express edition /Developer
	(any year version of 2016 /2017)	(any year version of 2016 /2017)	(any year version of 2016 /2017)	(any year version of 2016 /2017)
	Complete suite of SSDT or Visual Studio Professional	Complete suite of SSDT or Visual Studio Professional	Complete suite of SSDT or Visual Studio Professional	Complete suite of SSDT or Visual Studio Professional
Data source format	.csv or .txt	.csv or .txt	.csv or .txt	.csv or .txt /excel (.xlsx, .xls)

20. Formats of Annexures and Reports

Annexure 1

Format of declaration from DRM Vendor

(On DRM Vendor letterhead)

TO WHOMSOEVER IT MAY CONCERN

This is to certify that M/s _____ (DPO Name) _____ address: _____

_____ having its DAS headend at _____ has installed Digital Rights Management (DRM) from our company for its distribution network.

Date of DRM Installation and operational: _____ DRM Version: _____
 DRM ID (If any): _____ Network ID (If any): _____

Location and number of DRM servers (Database server, application server): _____

Details of main and back up DRM servers installed: _____ --

Any Database instance/split created, if yes please specify the no. of instances _____ and _____ date _____ of creation: _____

Number of DPOs/networks configured (applicable in case of infrastructure sharing)

Server time format:_____

Database detail:_____

Attached schematic diagram of DRM Systems installed in headend/remote/back up headend. And also the details and integration of distribution networks connected to the main headend (in case of infrastructure sharing).

With respect to the DRM installed at above mentioned headend and in terms of Schedule-X of the 'Interconnection Regulations', of TRAI, we confirm the following:

- Compliance to DRM Requirements mentioned in Table 1 under Schedule X.
- Compliance to DRM Requirements mentioned in Table 2 under Schedule X.
- Compliance to DRM Requirements mentioned in Table 3 under Schedule X.

I __(_name)_____ undertake that the information provided above is true and full disclosure of all the DRM system(s) provided to the said distributor has been made above and no information has been concealed.

Thanking you,
For (DRM company name)

(Signature)

Name :

Designation : (not below the level of COO or CEO or CTO)

Date :

Company seal :

Date: (within 90 days prior to audit)

Annexure 2

Format of declaration from SMS Vendor

(On SMS Company Letter Head)

Date:

TO WHOMSOEVER IT MAY CONCERN

This is to certify that M/s

_____, address: _____ having
its DAS headend at _____
has installed Subscriber Management System (SMS) from our company for
its distribution network.

Date of installation of SMS: _____

SMS Version: _____

Location of SMS servers: _____

SMS Database detail with number of instances/splits
created: _____

_____(Yes/NO)

If yes, then please specify the no. of instances/splits and date of creation:

Number of DPOs/network configured (in case infrastructure sharing):

Please find enclosed the schematic diagram of SMS and DRM system(s)
integration. And also the Number of DPOs/networks configured (in case
infrastructure sharing)_____

With respect to the SMS installed at above mentioned headend and in terms
of Schedule-X of the 'Interconnection Regulations', of TRAI, we confirm the
following:

- Compliance to SMS Requirements mentioned in Table I under Schedule X.

I __(_name)_____ undertake that the information provided above is true and
full disclosure of all the SMS system(s) provided to the said distributor has
been made above and no information has been concealed.

Thanking you,

For (SMS company name)

(Signature)

Name :

Designation : (not below the level of COO or CEO or CTO)/Authorised
signatory

Company seal :

Annexure 3

Format of Audit form to be filled in by DPO

(Compliance Audit Form)

On DPO Letter Head

(In the case of infrastructure sharing, a separate Compliance Audit Form shall be filled by each of the Infrastructure Seeker also.)²¹

Type of DPO: IPTV		Date :				
Address of the headend						
Headend technical person :Contact No. ..						
1	No..of SD & HD Channels presently running in the network		FTA	PAY	TOTAL	
		SD				
		HD				
Sl. No.	DRM Make	Version	For Software Application (Cardless)			Server Location
			Encryption Algorithm	Key Length		
1						
2						
Sl. No.	SMS Make	Version	Date of Installation		Server Location	
1						
2						
Sl. No.	STB Make (If applicable)	Model	(HD, SD, PVR)	Hybrid	Android	
1						
2						
3						
4						
5						
A) Digital Rights Management (DRM) & Subscriber Management System (SMS)		Yes/No				
1	Is the SMS computerized and capable to record the vital information and data concerning the subscribers such as:					
	a. Unique Customer Id					
	b. Subscription Contract number					
	c. Name of the subscriber					
	d. Billing Address					

²¹ This provision has been included keeping in view of the provisions of sharing infrastructure if amended in future.

	e. Installation Address		
	f. Landline telephone number		
	g. Mobile telephone number		
	h. Email id		
	i. Service/Package subscribed to		
	j. Unique STB Number		
	k. Unique VC Number		
2	Is the SMS able to undertake the following:		
	a. Viewing and printing historical data in terms of the activations, deactivations etc.		
	b. Location of each and every set top box VC unit		
	c. Generating historical data of changes in the subscriptions for each subscriber and the corresponding source of requests made by the subscriber.		
	i. The total number of registered subscribers.		
	ii. The total number of active subscribers.		
	iii. The total number of temporary suspended subscribers.		
	iv. The total number of deactivated subscribers.		
	v. List of blacklisted STBs in the system.		
	vi. Channel and bouquet wise monthly subscription report in the prescribed format.		
	vii. The names of the channels forming part of each bouquet.		
	viii. The total number of active subscribers subscribing to a particular channel or bouquet at a given time.		
	ix. The name of a-la carte channel and bouquet subscribed by a subscriber.		
	x. The ageing report for subscription of a particular channel or bouquet.		
3	Are SMS and DRM integrated for activation and deactivation process from SMS to be simultaneously done through both the systems? Is the DRM system independently capable of generating log of all activation and deactivations?		
4	Are SMS & DRM capable of individually addressing subscribers, on a channel by channel and STB by STB basis?	DRM	SMS
5	For VC based DRM, is the STB & VC paired from head-end to ensure security? (If applicable)		
6	Is DRM system provider able to provide monthly log of the activations on a particular channel or on the particular package?		

7	Is SMS able to generate itemized billing such as content cost, rental of the equipment, taxes etc?					
8	Do DRM & SMS have provision to tag and blacklist VC numbers and STB numbers that have been involved in piracy in the past to ensure that the VC or the STB/Software Application cannot be redeployed?	DRM		SMS		
9	Is DRM able to provide reports at any desired time about:					
	a. Active and De-active VC/Unique Consumer Subscription wise details as on any particular date					
	b. STB/Unique Consumer Subscription Activation / De-activation					
	c. Channels Assignment to STB/Unique Consumer Subscription					
	d. Report of the activations or the deactivations of a particular channel for a given period.					
10	Is DRM & SMS able to provide reports at any desired time about:	DRM		SMS		
	a. a. VC wise log of changes in packages/channels for any particular period					
	a. Logs of creation and modification of packages for any particular period					
11	Total No. of STBs deployed in the network presently?	In field SD: In field HD:				
B) Fingerprinting & Scroll messaging		STB1	STB2		STBN	Software Application
		Yes/No				
1	Is FP Facility available (Channel Specific/Global)					
	a. Visible (Overt)					
	b. Invisible (Covert))?					
2	Is the finger printing removable by pressing any key on the remote control / front panel of STB?					
3	Is the fingerprinting on the topmost layer of the video?					
4	Can the Finger printing identify the unique STB number or the unique Viewing Card (VC) number /Unique Consumer Subscription etc?					
5	Does fingerprinting appear on all the screens of the STB, such as Menu, EPG etc.?					
6	Is the location of the Finger printing changeable from the Headend and random on the viewing device?					
8	Is finger printing possible on global STB basis?					
	Is finger printing possible on individual STB/user basis?					

9	Is overt finger printing displayed by the MSO without any alteration with regard to the time, location, duration and frequency.					
10	Is the scroll messaging character length 120 or more?					
11	Does STB/Software Application has forced messaging capability?					
12	Is there provision for the global messaging, group messaging and the individual STB/Unique Consumer Subscription messaging?					
D) STB/Software Application		STB1	STB2	STB3	STB4	Software Application
		Yes/No				
1	Is Valid BIS certificate of each model of STB available? (if applicable)					
2	Does the STBs/Software application in Unique Consumer Subscription with facilities for recording the programs have copy protection system?					
3	Is STB/software application addressable to be upgraded by OTA?					
4	Watermark of the network logo is Encoder or STB/Software Application generated?					

I __(_ name)_____ undertake that the information provided above is true and full disclosure of all the DRM and SMS system(s) and STB/software application has been made above and no information has been concealed.

DPO Signature

(Signature)

Name :

Designation : (not below the level of COO or CEO or CTO)/Authorised signatory

Company seal :

Annexure 4

Format of declaration from STB

(On STB company letterhead)

TO WHOMSOEVER IT MAY CONCERN

This is to certify that M/s _____ (DPO Name) _____ address: _____

_____ having its IPTV headend at _____

has procured below mention STB model no from our company for its distribution network.

S. no	STB Model no	BIS Compliant (yes/No)	Date of BIS Certificate

All the STB deployed/purchased by DPO are in compliance to Schedule-X of the 'Interconnection Regulations'.

1. All STBs should have a DRM content protection.
2. The STB should be capable of displaying fingerprinting inserted from Headend through DRM/SMS.
3. The STB should support both targeted channel fingerprinting as well as all global fingerprinting.
4. The STB should be individually addressable from the IPTV Head-end.
5. The STB should be able to receive messages from the IPTV Head-end.
6. The messaging character length should be minimal 120 characters.
7. There should be provision for global messaging, group messaging and the individual STB messaging
8. The STBs should be addressable over the air to facilitate OTA software upgrade.
9. The STBs with facilities for recording the programs shall have a copy protection system.
10. STB/unique consumer subscription should take all commands directly from DRM not from any intermediate servers.

I __(_name)_____ undertake that the information provided above is true and full disclosure of all the STB(s) provided to the said distributor has been made above and no information has been concealed.

Thanking you,
For (STB company name)

(Signature)

Name :

Designation : (not below the level of COO or CEO or CTO)

Date :

Company seal :

Date:
(.....)

Annexure 5

Format of declaration from Software Application in user device by Vendor

(On Vendor letterhead)

TO WHOMSOEVER IT MAY CONCERN

This is to certify that M/s _____ (DPO Name) _____ address: _____

_____ having its IPTV headend at _____

has procured/developed below mention software application from our company.

S. N o	Software Application	Deployed in (TV/STB/Device type)	Version	Date of Deployment/Procurement

Note: Software Application vendor are also required to submit security audit testing certificate from CERT-IN empanelled agencies along with declaration certificate.

The software application purchased by DPO are in compliance to Schedule-X of 'Interconnection Regulations'.

1. All software application in user device should support DRM content protection.
2. The software application in user device should be capable of displaying fingerprinting inserted from Headend through DRM/SMS.
3. The software application in user device should support both targeted channel fingerprinting as well as all global fingerprinting.
4. The software application in user device should be individually addressable from the IPTV Head-end.
5. The software application in user device should be able to receive messages from the IPTV Head-end.
6. The messaging character length should be minimal 120 characters.

7. There should be provision for global messaging, group messaging and the individual STB messaging
8. The software application in user device should be addressable over the air to facilitate OTA software upgrade.
9. The software application in user device with facilities for recording the programs shall have a copy protection system.
10. The software application in user device subscription should take all commands directly from DRM not from any intermediate servers.

I __(_name)_____ undertake that the information provided above is true and full disclosure of all the STB(s) provided to the said distributor has been made above and no information has been concealed.

Thanking you,
For (STB company name)

(Signature)

Name :

Designation : (not below the level of COO or CEO or CTO)

Date :

Company seal :

Date:

(.....)

Annexure 6

Format of subscription audit form

(Letter head of DPO)

S.No	Area	Details	DPO Response
1	Head End	General Details	
1.1	Details	Headend Location	
1.2		Date of establishment of the Headend	
1.3		Number of digital headend/sub Headends with encryption details and areas covered	
2		Hardware Details (if it is not covered in network diagram of all DHE's)	
2.1		Details of IRD's with make & model number	
3		Others	
3.1		Local Channel detail:(number of local channels)	
3.2		Is a unique LCN defined for each channel (Service ID)	
3.3		Encryption:	
3.4		Watermarking:	
3.5		Is watermark inserted? If yes, from where?	
4	Subscriber Management System (SMS)	Features	
4.1		Make & version number	
4.2		Types of STB's used with make, model number & compatibility with DRM	
4.3		Software Application Details	
4.4		Modules in SMS & the activities performed for each of the module	
4.5		Audit/trail/log of all changes for all changes made to the customer account & STB	
4.6		Channels to package mapping	
4.7		Fingerprinting (STB/user wise, Group/All)	
4.8		Messaging (STB/user wise, Group/All)	
5		Reporting	
5.1		Is reporting module configured to extract the following reports:	
5.2		As on historical date, count and details of STB status (active/de-active) as per the system	
5.3		Count and details of Activation/ deactivation of STBs for a defined period	
5.4		STB/Account wise Package modification report for a defined period	
6	Digital Rights Management (DRM)	Features	
6.1		Number of DRM systems installed at the headend & the version of each	

6.2	Number of channels configured on each DRM	
6.3	Channel to package/product mapping	
6.4	Fingerprinting (STB/user wise, Group/All)	
6.5	Messaging (STB/user wise, Group/All)	
7	Reporting	
7.1	Is reporting module configured to extract the following reports:	
7.2	As on historical date, count and details of active STB/Unique Consumer Subscription status as per the system	
7.3	Activation and deactivation log for each STB/ VC Id/Unique Consumer Subscription	
7.4	Activation and deactivation log of channels and packages for each STB/VC ID/Unique Consumer Subscription	

Undertaking

I __(_name)_____ undertake that the information provided above is true, full and complete disclosure of all the DRM and SMS system(s) and STB/software application in user device has been made above and no information has been concealed.

(Signature)

Name :

Designation : (not below the level of COO or CEO or CTO)/Authorised signatory

Company seal :

Compliance Report of
Addressable System of
M/s _____
for conformity to Schedule X of the
Interconnection Regulations 2017
(as amended)

INDEX/TABLE OF CONTENTS

Contents

1 Introduction and Background.....	
1.1 Background of the DPO	
1.2 Terminologies used in Audit Report	
1.3 Headend Architecture	
1.3.1 Details of Broadcaster's IRD(s)	
1.3.2 Details of DRM(s)	
1.3.3 Details of SMS(s)	
1.3.4 Detail of the Signal Processing Systems	
1.3.5 LCN wise service details	
1.3.6 Package Configuration	
1.4 Network Architecture	
1.5 Set Top Box Management Process	
1.6 Consumer Acquisition Process	
1.7 Data Management Process	
2 Methodology Adopted for Compliance Audit	
3 Audit Details	
3.1 Audit Period & Locations	
4 Schedule X Compliance Report	
4.1 Compliance Report for DRM & SMS	
4.2 Compliance Report for DRM regarding encryption.....	
4.3 Compliance Report for 4.3 Finger Printing	
4.4 Compliance Report for STB/Software Application in Unique Consumer Subscription	
5 Auditor's Observations	
6 Auditor's Opinion & Conclusion	
7 Annexures of Pre-Signal/Compliance Audit Report	
(Note: Add relevant page numbers)	

Introduction and Background

Background of the DPO

[
Background on the DPO organization.
Brief detail of the business operation and experience on the cable TV distribution.
Details regarding the expansion of the DPO services
Annexure: Copy of valid license/ permission from MIB
]

Terminologies used in Audit Report

[
Explanation of terms used in the report but are not part of the Act/ Rules/ Regulations/ Guidelines
]

Headend Architecture

[
Explanation on the entire infrastructure of the DPO including Disaster Recovery Site for the operations.

Explanation of the following processes:

- i. Content Reception*
- ii. Content Proccession*
- iii. Encryption details*
- iv. Monitoring setup*
- v. Content reception at consumer premises*

Annexure: Copy of Headend Schematic Diagram

]

Details of Broadcaster's IRD(s)

[

List of Broadcaster's IRDs present at the headend and their operational status
]

Details of DRM(s)

[
Details of the DRMs installed

Detail of the licensed/authorized VC/STBs/Unique Consumer Subscription available in the respective DRM(s)
Details of Infrastructure Seekers in case of infrastructure sharing²²
]

Details of SMS(s)

[
Details of the SMS(s) installed

Detail of the SMS(s) installed with the respective DRM(s)
Details of Infrastructure Seekers in case of infrastructure sharing²³
]

Detail of the Signal Processing Systems

[
Details w.r.t. configurations of the following hardware in the network (at main/satellite / remote headends)

- i. DRM Servers*
- ii. Encryption server*
- iii. SMS servers*
- iv. Multiplexers*
- v. PSI/ SI servers*
- vi. CDN servers*
- vii. Fiber transmitters*

]

²² Amendment made in view of the provisions related to sharing of infrastructure.

²³ Amendment made in view of the provisions related to sharing of infrastructure.

LCN wise service details

[
List of the LCN-wise channels present on the EPG as well as content available on the screen (to be checked and recorded after assigning all the available services to the test STB/Unique Consumer Subscription)
]

Package Configuration

[
i. *Package-wise list and detail of services configured in SMS(s) as on date²⁴ of audit*
ii. *Package-wise list and detail of services configured in DRM(s) as on date of audit*
]

Network Architecture

[
Annexure: Copy of Network Diagram w.r.t. Main Headend / Remote Headends and integration of infrastructure seekers, in case of Infrastructure sharing²⁵
]

Set Top Box/User Management Process

[
Detail of the STB/user management system w.r.t. following:
i. *Authorization process of STB/ VC/user in DRMs,*
ii. *Transfer of STBs/ VCs from DPO to LCO and LCO to consumer*
iii. *Activation deactivation process of STB/user*
]

²⁴In Compliance audit, this data should be limited to as on date of audit keeping in view of the voluminous data related to package channel configuration in SMS and DRM.

²⁵ Amendment made in view of the provisions related to sharing of infrastructure.

Consumer Acquisition Process

[
Detail of the consumer acquisition process including allocation of the STB/VC, pairing of STB-VC and activation of packages/ services on the STB
Identification process of each STB in cases when multiple STB are assigned to single consumer
Activation process of User activation through Software Applications.

Data Management Process

[
Explanation of the system and procedure adopted by DPO for management of the data from DRMan and SMS deployed for the headend

Explanation may include details regarding:

- i. Servers*
- ii. Backup server/ Mirror server*
- iii. Reporting servers*
- iv. Etc.*

]

Methodology Adopted for Compliance Audit

[
Section will provide details of the audit team(s) and explanation of the procedure for compliance audit.

]

Audit Details

[[

Audit Period & Locations

[
Section will provide the audit period including no. of audit visits and duration of each visit and details of visit at remote site(s)
]

Schedule X Compliance Report

//

Compliance Report for DRM & SMS

[
*Section will cover point-wise compliance for the requirements w.r.t. DRM & SMS specified in the Schedule-X the 'Interconnection Regulations'.
(Ideally in tabular form)*
]

Compliance Report for DRM regarding encryption

[
*Section will cover point-wise compliance for the requirements w.r.t. DRM & SMS specified in the Schedule-X the 'Interconnection Regulations'.
(Ideally in tabular form)*

Compliance Report for Finger Printing

[
*Section will cover point-wise compliance for the requirements w.r.t. DRM & SMS specified in the Schedule-X of the 'Interconnection Regulations'.
(Ideally in tabular form)*
]

Compliance Report for STB/Software Application in Unique Consumer Subscription

[
Section will cover point-wise compliance for the requirements w.r.t. DRM & SMS specified in the Schedule-X of the 'Interconnection Regulations'.
(Ideally in tabular form)
]

Auditor's Observations

[
Section will cover point-wise explanation for any-compliance parameter OR any deviation OR any abnormality in the Addressable System w.r.t. the requirements specified in the Scope of work in the Audit Manual
(Ideally in tabular form)

Scope of Work	Status/ Observations
IP configuration to confirm and identify servers and mux deployed	
Inventory details of the Broadcasters IRDs+ VCs	
Record of PSI/ SI servers (for EPG and LCN)	
Watermarking provisions	
Encryption status of the channels/ services	
Compliance Status of the DRM & SMS	
Compliance Status of the Fingerprinting	
Compliance Status of the STBs/software Application in user Device deployed	
Analysis of VCs/Unique Consumer Subscription/ Ground Samples	

]

Auditor's Opinion & Conclusion

[
Section will provide the auditor's opinion and conclusion for the addressable system deployed by the DPO
]

Annexures of Pre-signal/compliance audit Report

[
Section will have the annexures as required and mentioned in the Audit Report
]

Subscription Audit Report of
verification carried out for conforming
the completeness, truthfulness and
correctness of

M/s..... for verification of
Monthly Subscription Reports (MSR)
submitted to <Name of Broadcaster>

by

M/s _____

Date of Issue:

INDEX/TABLE OF CONTENTS

Contents

1. Introduction and Background	
1.1 Background of the DPO	
1.2 Terminologies used in Audit Report	
1.3 Headend Architecture	
1.3.1 Details of Broadcaster's IRD(s)	
1.3.2 Details of DRM(s)	
1.3.3 Details of SMS(s)	
1.3.4 LCN wise service details	
1.3.5 Package Configuration	
1.4 Network Architecture	
1.5 Set Top Box/Unique Consumer Subscription Management Process.....	
1.6 Consumer Acquisition Process	
1.3.6 Data Management Process	
2. Methodology Adopted for Subscription Audit	
3. Audit Details	
3.1 Audit Period & Locations	
4 Subscription Audit	
4.1 List of <Name of the Broadcaster>'s channels distributed by the DPO.....	
4.2 Count of subscribers as derived by the auditor	
4.3 Total Count of Subscribers	
4.4 Subscriber Count of Channel 1 (Suggestive MSR Report Format)	
5. Auditor's Observations	
6. Auditor's Opinion & Conclusion	
7. Annexures of Subscription Audit Report	

(Note: Add relevant page numbers)

Introduction and Background

Background of the DPO

[
Background on the DPO organization.
Brief detail of the business operation and experience on the cable TV distribution.
Details regarding the expansion of the DPO services
Annexure: Copy of valid license/ permission from MoI&B
]

Terminologies used in Audit Report

[
Explanation of terms used in the report but are not part of the Act/ Rules/ Regulations/ Guidelines
]

Headend Architecture

[
Explanation on the entire infrastructure of the DPO including Disaster Recovery Site for the operations.

Explanation of the following processes:

- i. Content Reception*
- ii. Content Proccession*
- iii. Encryption details*
- iv. Monitoring setup*
- v. Content reception at consumer premises*

Annexure: Copy of Headend Schematic Diagram

]

Details of Broadcaster's IRD(s)

[

List of Broadcaster's IRDs present at the headend and their operational status
]

Details of DRM(s)

[
Details of the DRM(s) installed

Detail of the licensed/authorized VC/STBs available in the respective DRM(s)
]

Details of SMS(s)

[
Details of the SMS(s) installed

Detail of the SMS(s) installed with the respective DRMs
]

LCN wise service details

[
List of the LCN-wise channels present on the EPG as well as content available on the screen (to be checked and recorded after assigning all the available services to the test STB)
]

Package Configuration

[
i. Package-wise list and detail of services configured in SMS(s) for minimum 20% random selected dates of MSR verification²⁶.

²⁶ In subscription audit, this data should be limited to MSR verification dates only keeping in view the voluminous data related to package channel configuration in SMS and DRM.

- ii. *Package-wise list and detail of services configured in DRM(s) for minimum 20% random selected dates of MSR verification.*²⁷

]

Network Architecture

[

Annexure: Copy of Network Diagram w.r.t. Main Headend and Satellite/ Remote Headends

]

Set Top Box/ Unique Consumer Subscription Management Process

[

Detail of the STB management system w.r.t. Authorization process of STB/ VC/Unique Consumer Subscription in DRM,

Annexure: Flow Chart of the STB Management

]

Consumer Acquisition Process

[

Detail of the consumer acquisition process including allocation of the STB/VC/Unique Consumer Subscription, pairing of STB-VC and activation of packages/ services on the STB/Software Application

Identification process of each STB/Software Application in cases when multiple STB/Unique Consumer Subscription are assigned to single consumer

Annexure: Flow Chart of the Consumer Acquisition Process

]

Data Management Process

²⁷ In subscription audit, this data should be limited to MSR verification dates only keeping in view the voluminous data related to package channel configuration in SMS and DRM.

[
Explanation of the system and procedure adopted by DPO for management of the data from DRM and SMS deployed for the headend

Explanation may include details regarding:

- i. Servers*
- ii. Backup server/ Mirror server*
- iii. Reporting servers*
- iv. Etc.*

]

Methodology Adopted for Subscription Audit

[
Section will provide details of the audit team(s) and explanation of the procedure for Subscription audit.

Auditors are required to carry necessary check for verification of the integration of the DRM and SMS before conducting reconciliation and MSR verification.

]

Audit Details

//

Audit Period & Locations

[
Section will provide the audit period including no. of audit visits and duration
of each visit and details of visit at remote site(s)
]

Subscription Audit

//

List of <Name of the Broadcaster>'s channels distributed by the DPO

[
Auditor will provide the list of broadcaster's channels which are being distributed by the DPO OR were distributed by the DPO in entire duration of the audit
(Ideally in tabular form)
]

Count of subscribers as derived by the auditor

Total count of subscribers

Count as on XX.XX.XXXX	Count of VC/ STB			
	As per DRM	As per SMS	Present in SMS not in DRM	Present in DRM not in SMS
Active count²⁸				
DRM 1				
DRM 2				
DRM 3				

DRM N				

- VC to VC reconciliation for 5 minimum random Dates of Audit Period.
- Monthly State wise active account of subscribers for the audit period (Applicable for DPOs having operations in multiple States).

MSR Verification Table (Suggestive Format)

- It may be noted that in case system generated reports captures all the fields specified in the format, then the auditor may accept such system generated reports.
- In case of shared DRM architecture, or in case a DPO has multiple DRMs, the MSR verification can be done in such a manner where the total package/channel count of SMS needs to be reconciled with the total package/channel count of respective DRMs.

Subscriber Count of Channel 1 (Suggestive MSR Report Format)

As on XX.XX.XXXX (any of the randomly picked date from MSR)

Count as on XX.XX.XXXX	As per DRM	As per SMS	Reported MSR Count to Broadcasters	Variance (MSR- SMS)	----- % of Variation (Verified SMS Count vs Reported MSR Count)
A-la-carte Subscriptions					
Broadcaster's Package 1 Subscriptions					
Broadcaster's Package 2 Subscriptions					

Broadcaster's Package N Subscriptions					

[Section will MSR verification Report by selecting one random day for each month of audit Period]

Auditor's Observations

/

*Section will cover point-wise explanation for deviation in the count from MSR
(Ideally in tabular form)*

Scope of Work	Status/ Observations
<i>Observations on the Data Extraction Process</i>	
Observations on the Data Analysis	
Observations on the Channel to Package Mapping	
Observations and details of Test STB/ VCs	
Observations on the transaction logs	
EPG wise channel List	
Observations on analysis of TS Recordings	

/

Auditor's Opinion & Conclusion

[
*Section will provide the auditor's opinion and conclusion for the subscription
Audit of the IPTV System.*
]

Annexures of Subscription Audit Report

[
Section will have the annexures as required and mentioned in the Audit Report

Annexure 9

Format of Infrastructure sharing to be filled in by Infrastructure provider

(Signed and stamped on DPO Letter Head)

1. Number of Infrastructure seekers: _____
2. Total no of DRM.....
3. Total No of SMS.....
4. Attach seeker wise list of Pay TV IRD shared with each seeker (if any)

Details of Infrastructure seeker(s) sharing Headend							
S. No.	Total number of Headends	Details of Headend being shared			Name of the Infrastructure seeker	DoT/ authorisation MIB Registration No of Infrastructure seeker	Remark
		Headend Type (IPTV)	Location	Address			

Details of Infrastructure seeker(s) sharing DRM							
S. No.	DRM Name	Details of DRM being shared			Name of the Infrastructure seeker	DoT authorisation /MIB Registration No of Infrastructure seeker	Remark
		DRM Version	DRM Make	Address			

Details of Infrastructure seeker(s) sharing SMS							
S. No.	SMS Name	Details of SMS being shared			Name of the Infrastructure seeker	DoT authorisation /MIB Registration No of Infrastructure seeker	Remark
		SMS Version	SMS Make	Address			

Details of Infrastructure seeker(s) sharing MUX							
S. No.	MUX Type	Details of MUX being shared			Name of the Infrastructure seeker	DoT authorisation / MIB Registration No of Infrastructure seeker	Remark
		MUX Number	MUX Make	Address/ Headend Location			

Details of Infrastructure seeker(s) sharing Other Elements							
S. No.	Name of the element being shared	Details of Elements being shared			Name of the Infrastructure seeker	DoT authorisation/ MIB Registration No of Infrastructure seeker	Remark
		Number	Make	Address/ Headend Location			