Telecom Regulatory Authority of India

The Telecommunication (Broadcasting and Cable) Services Digital Addressable Systems Audit Manual

10 March 2026

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

In case of any comments regarding the manual, it may be sent to the following address:

Dr. Deepali Sharma,
Advisor (B&CS),
Telecom Regulatory Authority of India (TRAI),
World Trade Centre
4th, 5th, 6th & 7th Floor, Tower F,
Nauroji Nagar, New Delhi-110029, India
Email: advbcs-2@trai.gov.in

For any clarification/information, Advisor (B&CS) may be contacted at Tel. No.: +91-11-20907774.

INDEX

1. Background & Introduction

1.1 Keeping in view the implementation of Digital Addressable Systems (DAS) and effectively utilizing its benefits, Telecom Regulatory Authority of India (TRAI) after due consultation process brought out a common regulatory framework for digital addressable systems on 3rd March 2017. This framework comprises of the Interconnection Regulations, Quality of Service Regulations and Tariff Order for providing broadcasting services relating to television through digital addressable system.

1.2 The Telecommunication (Broadcasting and Cable) Services Interconnection (Addressable Systems) Regulations, 2017 dated 3rd March 2017 cover technical and commercial arrangements between Broadcaster & Distributor and Distributor & Local Cable Operators (LCOs) for providing television services to the consumers. The said regulations were further amended vide a notification dated 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 along with its amendments are hereinafter referred to as "Interconnection Regulations 2017"].

1.3 In the DAS based TV services value chain, a broadcaster uplinks signals of pay television channel to satellite in encrypted form. The distributor receives the signals from the satellite and decodes them using the decoder provided by the broadcaster. After processing and merging the TV Channel signals of multiple broadcasters, the distributor encrypts the combined signals and retransmits it further, either directly or through local cable operator, to customer. The distributor could be a Multi-System Operator (MSO), a Direct to Home operator (DTH), a Head-end in The Sky operator (HITS) or Internet Protocol Television (IPTV) operator.

1.4 The Interconnection Regulations 2017 provides for the Audit initiated by the Distribution Platform Operator (DPO) vide sub-Regulation (1) of Regulation 15 or by the Broadcaster vide sub-Regulation (7) of Regulation 10 and sub-Regulation (2) and (2A) of Regulation 15. The Audit of the systems of DPO is necessary to ensure that the equipment and the software (including configuration of systems) comply with the extant regulatory framework.

1.5 The regulations also provide for audit caused by a broadcaster, before the provisioning of signals to a new DPO as per sub-Regulation (7) of Regulation 10. Broadcaster caused audit could also occur as per sub-Regulation (2) and (2A) of Regulation 15.

1.6 The Telecommunication (Broadcasting and Cable) Service Interconnection (Addressable Systems) Regulations, 2017 and its subsequent amendments, are accessible on TRAI website www.trai.gov.in.

1.7 The Authority had issued a consultation paper on 'Empanelment of Auditors for Digital Addressable Systems' on 22nd December 2017. As a matter of practice and following a transparent process an open house discussion (OHD) on the above-mentioned consultation paper was convened on 12th April 2018 in Delhi. One of the suggestions received from some stakeholders was to develop a comprehensive audit manual for auditors to audit digital addressable systems. Further, it was also suggested that in addition to other aspects the said audit manual may consist of a well-defined audit procedure.

1.8 Accordingly, the Authority constituted a committee comprising of industry stakeholders to prepare and submit draft Audit manual to the Authority. After extensive deliberations, the industry reached consensus on most of the issues barring few issues and submitted a draft audit manual to the Authority.

1.9 Based on the committee report and after considering all objections/representations, the Authority issued a consultation paper on 'The Telecommunication (Broadcasting and Cable) Services Digital Addressable Systems Audit Manual' on 29th March 2019.

1.10 After following a due consultative process, TRAI issued the Telecommunication (Broadcasting and Cable) Services Digital Addressable Systems Audit Manual[1] on 8th November 2019 [hereinafter called Audit Manual 2019].

1.11 Over time as the industry gained experience in conducting audits of DAS, various stakeholders of the industry including Broadcast Engineering Consultants India Limited (BECIL), and the Auditors empaneled by TRAI have suggested that certain amendments/modifications are required in the existing Audit Manual

[1] https://trai.gov.in/sites/default/files/2024-09/Audit_manual_08112019_0.pdf

2019 and Schedule III of the Interconnection Regulation 2017. Some service providers have raised need for incorporating amendments in the regulation and audit manual post infrastructure sharing guidelines for MSOs dated 29th December 2021, for HITS dated 06th November 2020, and for DTH dated 16th September 2022, issued by the Ministry of Information and Broadcasting (MIB). Therefore, it is required to identify issues in the existing Interconnection Regulation 2017 and Audit manual 2019 that may require amendments for enabling infrastructure sharing amongst service providers and audits post such infrastructure sharing. Also, there was an imminent need to streamline audit mechanism to increase accountability of auditors and reduce unnecessary re-audits.

1.12 Accordingly, TRAI issued a consultation paper on 'Audit related provisions of Telecommunication (Broadcasting and Cable) Services Interconnection (Addressable Systems) Regulations, 2017 and the Telecommunication (Broadcasting and Cable) Services Digital Addressable Systems Audit Manual' on 9th August 2024 (hereinafter referred to as the "consultation paper") for seeking comments of the stakeholders. Comments and counter comments received from stakeholders were placed on TRAI's website. This was followed by an open house discussion on 5th December 2024.

1.13 After following a due consultative process, TRAI issued the Telecommunication (Broadcasting and Cable) Services Interconnection (Addressable Systems) (Seventh Amendment) Regulations, 2026 on 5th February 2026 (hereinafter referred to as the "Seventh Amendment Regulations").

1.14 After duly considering all the comments and counter-comments received from the stakeholders in response to the consultation paper and its own analysis, the Authority has finalized the 'Telecommunication (Broadcasting and Cable) Services Digital Addressable Systems Audit Manual, 2026' [hereinafter called Audit Manual] and shall come into force from 1st April 2026.

1.15 This audit manual addresses issues related to DAS audits in terms of Regulations 10 and 15 of the Interconnection Regulations 2017.

1.16 During the course of conduct of audit, necessity of modifications in this manual may arise due to technological/techno-commercial changes, market development and changes in the systems, etc. The Authority may notify such modifications which shall come into effect from the date as prescribed in the notification.

1.17 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 2017, other extant Regulations or Tariff Order and the Audit Manual, the provisions as per the regulations/tariff Orders shall prevail.

1.18 The audits provisioned under the Interconnection Regulations 2017 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.trai.gov.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. 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 otherwise it will be called as compliance audit. It may be noted that pre-signal/compliance audit will be carried out as per Schedule III mentioned in the Interconnection Regulations 2017.

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 addressable systems to be used for distribution of television channels meet the requirements as specified in the Schedule III of the Interconnection Regulations 2017. 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 agency empanelled by TRAI or BECIL as per Schedule III under sub-regulation (6) of regulation 10 of the Interconnection Regulations 2017. 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 of the Interconnection Regulations 2017 and the DPO may provide its declaration in writing to broadcaster regarding Schedule III compliance along with below mentioned documents for requesting signals.

- CAS certificate provided by vendor.
- SMS certificate provided by vendor.
- STB certificate provided by vendor.
- BIS compliance certificate.

2.4 Sub-regulation (7) of Regulation 10 of the Interconnection Regulations 2017 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 of the Interconnection Regulations 2017, it may, cause audit of the addressable system of the distributor by M/s. Broadcast Engineering Consultants India Limited (BECIL), or any other auditor empanelled by the Authority for conducting such audit 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)[2] of Regulation 10, before instituting such audit by the broadcaster.

2.5 The proviso to the said Regulation provides for the case where the system of the distributor has been successfully audited (with full compliance) during the last one year by M/s. Broadcast Engineering Consultants India Limited (BECIL), or any other auditor empanelled by the Authority. 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 addressable system requirements

[2] 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.*"

as per Schedule III of the Interconnection Regulations 2017. 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 2017, 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. The annual audit caused by distributor shall include the audit to validate compliance with the Schedule III of the Interconnection Regulations 2017 and the subscription audit, as provided for in the Interconnection Regulations 2017. The above annual compliance audit will also be applicable in case of infrastructure sharing.[3]

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 (CAS, 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 2017, 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***

[3] This amendment is required to cover infrastructure sharing.

b) Change in the SMS version w.r.t last audited SMS
c) Addition/Deletion of CAS
d) Change in the CAS version w.r.t last audited CAS
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[4].

2.10 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.

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 2017. As mentioned earlier, as per sub-regulation (1) of Regulation 15, the annual audit caused by distributor shall include the audit to validate compliance with the Schedule III of the Interconnection Regulations 2017 and the subscription audit, as provided for in the Interconnection Regulations 2017. 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 2017 (or in case of pre-signal audit, after taking into consideration the proviso to sub regulation 7 of Regulation 10).

[4] Keeping in view the provisions of sharing infrastructure point 'f' is added.

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 including MUX.

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 DPO[5].

4.5 Check Multiplexer (MUX) configuration to validate number of Transport Streams ("TS") configured with Service Identifier (SID), scrambling status of each SID and Entitlement Control Message (ECM) and Entitlement Management Message (EMM) configuration (MUX-TS Stream-No. of ECM & EMM configured). In case of Infrastructure sharing the MUX deployed should be capable of providing a differentiator to identify TS streams shared between multiple DPOs which can be validated during audits or separate MUX needs to be deployed for each entity sharing infrastructure[6].

4.6 Take screenshot of all TS streams from MUX and compare with results of field TS recorded randomly at minimum two locations by auditor. It may be noted that in case of multiple headends of DPO, TS verification needs to be carried out at each headend and respective field locations.[7]

4.7 Take information of Quadrature Amplitude Modulators (QAMs) installed and powered to identify streams available for local insertion by DPO and/or local cable operators (LCOs).

[5] 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.

[6] The above modification is essential in case of infrastructure sharing to ensure the validation of TS streams. Further, it will also ensure more transparency in the audit process.

[7] The above clause is modified to elaborate the existing requirement to ensure audit efficacy and transparency.

4.8 Obtain record of Program Specific Information/Service Information (PSI/SI) server to confirm Electronic Programme Guide (EPG), Logical Channel Number (LCN) etc. details.

4.9 Check PSI/SI server that it has EPG push capability.

4.10 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.

4.11 Use Free to Air (FTA) cable box/ TS analyzer to confirm whether all channels are encrypted.

4.12 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.

4.13 Verification of compliance of Schedule III of the Interconnection Regulations 2017 of the DPO’s DAS System (CAS, SMS, Fingerprinting and STB) as per procedure mentioned in section 7 of the Audit Manual.

4.14 Data Extraction from CAS and SMS should be carried out as per requirements specified in Schedule III of the Interconnection Regulations 2017. Procedure and method of data extraction is specified in the section 7 and section 16 of the Audit Manual.

4.15 Report the channels found running in unencrypted or analogue mode on the day of Audit.

4.16 Analysis and verification of TS recording/VC samples 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.

4.17 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 provider[8].

- 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 CAS/SMS or both.

In the case of sharing of CAS/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.

5. Documents required under pre-signal/ Compliance audit

5.1 Valid DAS license/permission issued by Ministry of Information and Broadcasting (MIB).

5.2 BIS certificates for all makes & models of STB deployed by DPO after DAS implementation.

5.3 Certificate from all the CAS vendors (Format as in **Annexure 1**).

5.4 Certificate from SMS vendors (Format as in **Annexure 2**).

[8] 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 CAS, 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.

5.5 Block Schematic diagram of Head-end including CAS 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**). It may be noted that the STB Vendor declarations would need to be provided only from those STB Vendors whose STBs have been deployed and activated by the DPO post coming into effect of the Interconnection Regulations 2017 i.e. from 29th December 2018 and who are still providing the support to DPOs. If DPO does not have a current business relationship with a STB vendor, then certificate issued from such STB vendor at the time of procurement should be acceptable[9].

5.8 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 DPO[10].

5.9 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 reports[11].

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 TS recordings and VCs (if any) for verification during audit and will share the same with auditors before the conduct of audit.

[9] Taking a STB vendor declaration by DPO from STB vendor with no existing business relationship is difficult and often not possible. The above amendment will help to address this issue.

[10] Some DPOs receive broadcasters' signal through decoders provided by them and some DPOs use PIRD with CAM to receive the signals, hence the clause 5.8 has been amended. 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.

[11] 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.

6.3 If the compliance audit is caused by broadcaster, in such cases broadcaster may share the TS recording/VC numbers (if any) with auditors for verification during conduct of audit.

6.4 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.

6.5 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.

6.6 The auditor will also share the documents requirements with DPO as specified in section 5 of the audit manual.

6.7 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.

6.8 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 headends of DPO where the CAS and SMS servers are installed.

6.9 The audit for compliance to Schedule III of the Interconnection regulations 2017 should be carried out by auditor as per procedure specified in section 7 of the Audit Manual.

6.10 The data extraction from CAS and SMS under compliance audit should be carried out as per section 7 of the Audit Manual.

6.11 The auditor will prepare the pre-signal/compliance audit report as per format provided in **Annexure 6** of the Audit Manual.

6.12 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.

6.13 If the audit is caused by the broadcaster, then the auditor will share the audit report copies both with broadcaster as well as DPO.

6.14 In case the audit report is non-compliant to the Interconnection Regulations 2017 then action may be taken as per sub-regulation (2B) of Regulation 15 of the Interconnection Regulations 2017.

7. Procedure to be followed for inspection of Schedule III of the Interconnection Regulations 2017

A. CAS and SMS requirements as per Schedule III of Interconnection Regulations 2017

It may be noted that all simulations tests on STBs should be carried out on those STB models that have been deployed and activated by the DPO post coming into effect of the Interconnection Regulations 2017. For this purpose, DPO must ensure that at least 2 STBs of each STB model, that have been deployed and activated by the DPO from 29th December 2018, are available in the stock for the simulation tests (if the STBs have not been audited earlier).[12]

Sl. no	Regulatory Provision	Audit Procedure
1	**Schedule III – C 1** The distributor of television channels shall ensure that the current version of the CAS, in use, do not have any history of hacking.	i. DPO to declare on its audit form the no. of CAS systems deployed in each of its distribution networks. It should mention the no. of 'Headend' connected with the said CAS. This declaration is required to be signed by the authorized signatory/compliance officer. **(Annexure 3)** ii. DPO to provide certificate from each CAS vendor on CAS vendor letterhead signed by no less than Authorized Signatory/Compliance Officer of the CAS vendor (Issued within last 12 months and certify current operating version of CAS) **(Annexure 1).**

[12] The above-mentioned amendment will save audit time as there is no need to test those STBs that have already been audited earlier. Further, year is changed from 2017 to 29th December 2018 since the implementation date of above regulations is 29th December 2018.

Sl. no	Regulatory Provision	Audit Procedure
		iii. Auditor to perform TS recording: i) At the Headend; ii) In the field at appropriate place. Auditor to analyze the TS streams to ascertain actual number(s) of CAS running in the network and compare with the declaration of CAS systems made to auditor before the conduct of audit[13]. Auditor to record discrepancy, if any. DPO should sign the record wherein Auditor has noted the discrepancy, if any. In case DPO refuses to sign, the Auditor should record the same.
2	**Schedule III – C 2** The SMS shall be independently capable of generating, recording, and maintaining logs, for the period of at least immediate preceding two consecutive years, corresponding to each command executed in the SMS including but not limited to activation and deactivation commands.	a) To check the availability of transaction logs in SMS for the period of last 2 years and analyze activation, de-activation, fingerprinting, messaging, blacklisting etc. b) DPO to certify on its letterhead the number of SMS deployed along with its integration status with all the CAS deployed. c) DPO to provide declaration from SMS vendor on SMS vendor letterhead (not older than 6 months) signed by no less than Authorized Signatory/Compliance Officer of the SMS vendor (**Annexure 2**). d) The above SMS certificate **(Annexure 2)** should mention DPO name & address matching with name & address mentioned in DPO registration certificate issued by Ministry of Information and Broadcasting. e) Auditors to check system capability for generating historical transaction logs along with date and time stamp. f) Auditor to check, verify and document whether all the actions, including but not

[13] The verifications vis-à-vis Broadcaster's signed agreement should be carried out by the broadcasters against the audit report received by them. Further, new systems might have been deployed by the DPO after signing of an agreement, and the audit report will duly capture the same in any case. Auditor should only record and report discrepancies (if any) between the CAS systems declared by the DPO in Compliance Audit Form and the same observed in the TS Recorded from DPO's Headend and Network.

Sl. no	Regulatory Provision	Audit Procedure
		limited to activation, de-activation, package creation, package change/modification, FP insertion, and scroll insertion are being recorded in SMS. In case of Infrastructure sharing of SMS between two or more DPOs the same should be applicable however the SMS should also be capable of generating instance/entity wise logs for the period prescribed above.[14]
3	**Schedule III – C 3** It shall not be possible to alter the data and logs recorded in the CAS and the SMS.	Simulation test should be carried on one model of every STB available in the inventory of DPOs for all actions such as subscriber creation, activation–de-activation, channel assignment, fingerprinting, messaging, scrolling through SMS. The logs of these activities then are required to be cross checked both in CAS and SMS live systems and whether these can be edited or not. It is clarified here that non editable requirement of SMS and CAS logs should be checked through live systems only. Once extracted or downloaded to any format these logs can be editable.
4	**Schedule III – C 4** The distributor of television channels shall validate that the CAS, in use, do not have facility to activate and deactivate a Set Top Box (STB) directly from the CAS terminal. All activation and deactivation of STBs shall be done	a) DPO to provide declaration and demonstrate procedures that all activations and deactivations of a Set Top Box (STB) directly from the CAS terminal are not done as a part of normal business operations. All activation and deactivation of STBs is done through SMS, except for internal testing purposes. b) Auditor on sample basis can check by trying to activate some STBs directly from the CAS and record the findings.

[14] In case of infrastructure sharing between DPOs, this will ensure transparency and help in conducting audits of DPOs sharing SMS.

Sl. no	Regulatory Provision	Audit Procedure
	with the commands of the SMS.	
5	**<u>Schedule III – C 5</u>** The SMS and the CAS should be integrated in such a manner that activation and deactivation of STB happen simultaneously in both the systems.	Auditor should perform simulation testing on one STB of every model deployed (if available in the inventory of DPO) as per following process: i) Activate different channels / packages on all test STBs from SMS. ii) Check transaction logs in SMS server and CAS server to confirm the activities related to channel activation and other simulation tests carried out reflects in both SMS and CAS logs with same date & time. It may be noted that the time delay due to server (CAS/SMS) load may be taken into consideration while carrying out the audit checks[15]. iii) Auditor should perform as on date unique VC Level Reconciliation from the data dump of CAS and SMS. VCs active in CAS but not in SMS and similarly VCs active in SMS but not in CAS should be highlighted as discrepancy.
6	**<u>Schedule III – C 6</u>** The distributor of television channels shall validate that the CAS has the capability of upgrading STBs over-the-air (OTA), so that the connected STBs can be upgraded.	Auditor to check that the CAS declaration **(Annexure 1)** confirms the availability of this facility.

[15] The systems (CAS and SMS) being dynamic in nature and activations and deactivation are done frequently, therefore some variance may be seen due to time delay. This may be taken into consideration while carrying out the audit checks.

Sl. no	Regulatory Provision	Audit Procedure
7	**Schedule III – C 7** The fingerprinting should not get invalidated by use of any device or software.	a) Auditor should trigger a fingerprint (any one ECM/EMM) of minimum 180 seconds duration from SMS/CAS to the test STB (minimum 180 seconds timeline is to ensure that fingerprinting command is still available on STB when it is rebooted as some of the STB takes at least 120 seconds to reboot). b) In case the CAS does not have provisions to send minimum 120 seconds FP then multiple commands of FP of short duration may be sent to verify the same. c) The STB should be rebooted, and fingerprint should reappear again automatically. If fingerprint disappears, auditor should take appropriate note.
8	**Schedule III – C 8** The CAS and the SMS should be able to activate or deactivate services or STBs of at least five percent (5%) of the subscriber base of the distributor within 24 hours.	Auditor should check CAS declaration **(Annexure 1)** and SMS declaration **(Annexure 2)** that mentions this capability.
9	**Schedule III – C 9** The STB and Viewing Card (VC) shall be paired from the SMS to ensure security of the channel.	a) Auditor should verify that paired VC of one STB should not work with another STB. b) Auditor to interchange VC between two STBs of the DPO and confirm that both STBs give error message on-screen. c) Auditor should take screenshot of the error message and include in audit report. d) Only applicable in case of card STBs.

Sl. no	Regulatory Provision	Audit Procedure
10	**<u>Schedule III – C 10</u>** The CAS and SMS should be capable of individually addressing subscribers, for the purpose of generating the reports, on channel by channel and STB by STB basis.	Auditor should: a) Activate fresh STBs individually through SMS and verify whether the same is activated in CAS as well. b) Add existing packages and channels to the test customer created through SMS and verify channels were activated in CAS and are visible on TV monitor. c) Remove packages/channels through SMS allotted to the test STB. d) After completing all other audit tests deactivate the test STB through SMS. e) Extract the logs of SMS and CAS for the day to check whether the above commands related to activation, deactivation of customer and packages were captured with date and time stamp.
11	**<u>Schedule III – C 11</u>** The SMS should be computerized and capable of recording the vital information and data concerning the subscribers such as: (a) Unique customer identification (ID) (b) Subscription contract number (c) Name of the subscriber (d) Billing address	Auditor should: a) Create at least two test customers in SMS with names - "AuditTest1Customerddmmmyy", "AuditTest2Customerddmmmyy". b) Allocate fresh hardware and map the test customer to an LCO/ DPO. c) Check whether item "(a) to (k)" specified in Schedule-III C 11 are getting captured (Auditor to provide details for filling the CAF). d) Take SMS screenshot(s) such that all items are covered. e) Generate SMS customer details report state wise and check the fields "a to k" are appearing. f) Auditor to deactivate the test subscribers from the SMS and confirm the corresponding STB is deactivated for all channels / services.

Sl. no	Regulatory Provision	Audit Procedure
	(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 (k) Unique VC number	g) Sample verification of 5 CAF forms selected randomly from the list of customers activated in last one month.
12	**<u>Schedule III – C 12</u>** The SMS should be capable of: (a) Viewing and printing of historical data in terms of the activations and the deactivations of STBs. (b) Locating each and every STB and VC installed. (c) Generating historical data of changes in the subscriptions for each subscriber and the	Auditor should ensure: a) Date & time stamp is mandatory in report generation. b) All data from SMS server should be extracted in such a manner that no STB/VC is left out from the database. c) In case the Auditor has reason to doubt the output from the SMS/CAS reporting modules, he may verify the output of the frontend with that of the backend of SMS/CAS. For this purpose, the Auditor may choose to run any query/code of the SMS/CAS vendor for the extraction of data as needed post verification of the query/code in terms of the filters being used and in terms of the entire database being referenced or not[16].

[16] Provision amended in view of data security and privacy concerns on including the screenshots of database structure and queries in the audit report. This will ensure transparency in audit procedure in case the outcomes of the SMS and CAS systems are compromised.

Sl. no	Regulatory Provision	Audit Procedure
	corresponding source of requests made by the subscriber.	In this regard, data extraction can be performed by the DPO in front of the auditor in case there are any doubts regarding the CAS and SMS systems. The DPO can operate/run commands on the systems in the presence of auditors while the auditors can watch/observe and note discrepancies (if any) in the audit report.[17]
13.	**<u>Schedule III – C 13</u>** The SMS should be capable of generating reports, at any desired time about: (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 in the system. (f) Channel and bouquet wise monthly subscription report	d) The Auditor will check the generation capability of these reports in SMS at any desired time from the front end (SMS application) of the SMS. e) The SMS reports generated during the audit exercise for verification will be enclosed with audit report as Annexures. f) The auditor on sample basis will also generate three reports from the SMS database (back end) and verify these reports with the reports generated from SMS application. g) It should be clarified here that auditor will not insist on any specific format of the reports generated from the front end (SMS application) or back end (SMS database) of the SMS However the report should be able to reflect desirable information.

[17] The method for conducting this audit procedure is elaborated to avoid any ambiguity. Data extraction cannot be performed directly by auditor on DPO CAS and SMS because a) auditor may not have the correct knowhow of the procedure and b) auditor may run any command which may disrupt DPO CAS and SMS. Therefore, any such exercise needs to be carried out by the DPO/vendor in front of the auditor in case there are any doubts regarding the CAS and SMS. This is because IP credentials system ID and passwords cannot be shared with any external teams by CAS/SMS vendors due to security reasons. Therefore, DPO can operate/run commands on the systems in the presence of auditors while the auditors can watch/observe, they cannot access the live systems themselves.

Sl. no	Regulatory Provision	Audit Procedure
	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.	
14	**<u>Schedule III – C 14</u>** The CAS shall be independently capable of generating, recording, and maintaining logs, for the period of at least immediate preceding two consecutive years, corresponding to each command executed in the CAS including but not limited to activation and deactivation	Auditor should ensure: a) Date & time stamp should be captured in all the reports generated from CAS. b) Auditor to extract historical transactional logs from CAS for audit period and confirm the availability of the data required. c) All data from CAS server (CAS servers installed by DPO and it's JVs CAS (including standby headends, mini headends) should be extracted in such a manner that no STB/VC is left out from the database. d) In case the Auditor has reason to doubt the output from the SMS/CAS reporting

Sl. no	Regulatory Provision	Audit Procedure
	commands issued by the SMS.	modules, he may verify the output of the frontend with that of the backend of SMS/CAS. For this purpose, the Auditor may choose to run any query/code of the SMS/CAS vendor for the extraction of data as needed post verification of the query/code in terms of the filters being used and in terms of the entire database being referenced or not[18]. In this regard, data extraction can be performed by the DPO in front of the auditor in case there are any doubts regarding the CAS and SMS systems. The DPO can operate/run commands on the systems in the presence of auditors while the auditors can watch/observe and note discrepancies (if any) in the audit report[19]. e) **Annexure1** should mention that CAS logs are available for up to preceding two consecutive years for each command executed in the CAS or from the date of installation of CAS at the headend if CAS is not 2 years old.[20] f) In case of infrastructure sharing, the auditor shall ensure that each CAS instance will communicate to one SMS or separate instance of SMS only. It should not be allowed that a common CAS instance to be addressed by multiple SMSs to refrain from reconciliation issues w.r.t. subscription nos. between CAS and SMS[21].

[18] This will ensure transparency in audit procedure in case the outcomes of the SMS and CAS systems are compromised.

[19] The method for conducting this audit procedure is elaborated to avoid any ambiguity. Data extraction cannot be performed directly by auditor on DPO CAS and SMS because a.) Auditor may not have the correct knowhow of the procedure and b) auditor may run any command which may disrupt DPO CAS and SMS. Therefore, any such exercise needs to be carried out by the DPO/vendor in front of the auditor in case there are any doubts regarding the CAS and SMS. This is because IP credentials system ID and passwords cannot be shared with any external teams by CAS/SMS vendors due to security reasons. Therefore, DPO can operate/run commands on the systems in the presence of auditors while the auditors can watch/observe, they cannot access the live systems themselves.

[20] The above audit manual procedure is modified to cover the scenario if the CAS is less than 2 years old.

[21] The above audit procedure is added to cover the scenario of infrastructure sharing.

Sl. no	Regulatory Provision	Audit Procedure
15	**<u>Schedule III – C 15</u>** The CAS shall be able to tag and blacklist VC numbers and STB numbers that have been involved in piracy in the past to ensure that such VC or the STB cannot be re-deployed.	a) Auditor to blacklist one STB & VC of each CAS (separate from test STB & VC) from SMS, and check the status of the STB+VC in CAS and SMS. b) Auditor to take logs of blacklisted STB +VC from CAS and SMS. c) Take screenshot of the blacklist screen to record the above and include in the report. d) If any STB of DPO has been blacklisted during audit for verification purpose, the same STB should be considered by auditor during re-audit caused by broadcaster unless broadcaster has any objections in respect of blacklisting capabilities of SMS and CAS deployed by DPO.
16	**<u>Schedule III – C 16</u>** It shall be possible to generate the following reports from the logs of the CAS: (a) STB-VC Pairing / De-Pairing (b) STB Activation / De-activation (c) Channels Assignment to STB (d) Report of the activations or the deactivations of a	Auditor will generate these reports from the CAS and would verify the same by generating these reports from SMS transactions log a) STB VC pairing de-pairing report is applicable only for carded CAS. b) Auditor shall keep screenshots of each report with masking of customer confidential data of DPO and include in the report. c) All data from CAS server to be extracted in such a manner that no STB/VC is left out from the database d) It should be clarified here that auditor will not insist on any specific format of the reports generated from the CAS application or from CAS server. However, the report should be able to reflect and produce desirable information.

Sl. no	Regulatory Provision	Audit Procedure
	particular channel for a given period.	
17	**<u>Schedule III – C 17</u>** The SMS shall be capable of generating bills for each subscriber with itemized details such as the number of channels subscribed, the network capacity fee for the channels subscribed, the rental amount for the customer premises equipment, charges for pay channel and bouquet of pay channels along with the list and retail price of corresponding pay channels and bouquet of pay channels, taxes etc.	On sample basis, Auditor to verify the Itemized bill generated from the SMS to ensure that it captures all the mentioned details in this clause & record a copy of the bill format & any discrepancy noticed, if any, in the audit report.
18	**<u>Schedule III – C 18</u>** The distributor shall ensure that the CAS and SMS vendors have the technical capability in India to maintain the systems on 24x7 basis throughout the year.	a) Auditor to check that the CAS declaration from each CAS vendor **(Annexure 1)** mentions the availability of this facility. b) Auditor to check that the SMS declaration **(Annexure 2)** from each SMS vendor mentions the availability of this facility.

Sl. no	Regulatory Provision	Audit Procedure
19	**Schedule III – C 19** The distributor of television channels shall declare the details of the CAS and the SMS deployed for distribution of channels. In case of deployment of any additional CAS/ SMS, the same should be notified to the broadcasters by the distributor.	a) DPO to declare on its letterhead the no. of CAS systems and SMS deployed in each of its distribution networks. It should mention the no. of "Headends" connected with the said CAS and SMS. This declaration is to be signed by authorized signatory/compliance officer. **(Annexure 3)** b) Any changes in CAS and SMS and STB should be reported by DPO and can be verified by auditor.
20	**Schedule III – C 20** Upon deactivation of any subscriber from the SMS, all program/services shall be denied to that subscriber.	Auditor to deactivate the "test subscribers" from the SMS and confirm the corresponding STB is deactivated for all channels/services including DD channels.
21	**Schedule III – C 21** The distributor of television channels shall preserve unedited data of the CAS and the SMS for at least two years.	a) In case of distribution platforms operational for less than 2 years, the Auditor to check that the CAS declaration from each CAS vendor **(Annexure 1)** mentions the CAS is compliant with this requirement. b) In case of distribution platforms operational for less than 2 years, the Auditor to check that the SMS declaration **(Annexure 2)** from each SMS vendor mentions the SMS is compliant with this requirement. c) Auditor to take declaration from DPO that it has preserved unedited data of the CAS and the SMS for at least two years if the CAS and SMS system are operational for more than 2 years. **(Annexure 3)**

SMS and CAS should have capability to meet all the requirements of each distributor as specified in schedule III of the Interconnection Regulation 2017. Further, separate instances should be created for each distributor using shared SMS/CAS 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 CAS.

B. Fingerprinting:

S. no	Regulatory Provision	Audit Procedure
1	**Schedule III – D1** The distributor of television channels shall ensure that it has systems, processes and controls in place to run fingerprinting at regular intervals.	a) Auditor to trigger fingerprinting from SMS/CAS[22] by inputting start/end time, duration of display, frequency of display and confirming that the fingerprint is seen on the test STB output. b) Auditor to take a screenshot of the fingerprint. For multiple fingerprinting tests on multiple STBs, the screenshots may be enclosed on sample basis.[23] It may be noted that fingerprinting may be triggered either from CAS or from SMS.[24]
2	**Schedule III – D2** The STB should support both visible and covert types of finger printing. The fingerprinting should not get invalidated by use of any device or software.	a) For visible type of finger printing: same as 1 above. b) For covert type: Auditor should ensure this capability is mentioned in STB certificate **(Annexure 4)** and as well test the same feature during audit. c) Auditor should accept any type of covert fingerprinting.

[22] Fingerprinting can be triggered either from CAS or from SMS since the end objective can be achieved both with CAS and SMS, this flexibility should be allowed from both the systems.

[23] It has been brought to the notice of TRAI that some broadcasters seek screenshots of each and every fingerprinting test performed on STBs during simulation testing during audit. Multiple tests are carried out during simulation tests and taking screenshot of each and every fingerprinting test is a time-consuming exercise. Additionally logs of simulations testing are also extracted from SMS and CAS as proof. Therefore, taking these many screenshots are not required. Further, auditor is required to ensure and satisfy that the outcome of all the simulation tests comply to regulatory requirement. The sample screenshots should be placed as artifacts in the report.

[24] Fingerprinting can be triggered either from CAS or from SMS since the end objective can be achieved both with CAS and SMS, this flexibility should be allowed from both the systems.

S. no	Regulatory Provision	Audit Procedure
	Provided that only the STB deployed after coming into effect of the Amendment Regulations shall support the covert finger printing.	**Note:** Only the STB deployed after coming into effect of the Amendment Regulations shall be required to support the covert finger printing. For multiple fingerprinting tests on multiple STBs, the screenshots may be enclosed on sample basis. If auditor is not able to capture the screenshots of covert FP, in that case screenshots of covert FP provisioning/logs through CAS/SMS should be taken.[25]
3	**<u>Schedule III – D 3</u>** The fingerprinting should not get invalidated by use of any device or software.	a) Auditor should trigger a fingerprint (any one ECM/EMM) of minimum 180 seconds duration from SMS/CAS to the test STB (minimum 180 seconds timeline is to ensure that fingerprinting command is still available on STB when it is rebooted as some of the STB takes at least 120 seconds to reboot). b) In case the CAS does not have provisions to send minimum 120 seconds FP then multiple commands of FP of short duration may be sent to verify the same. d) The STB should be rebooted, and fingerprint should reappear again automatically. If fingerprint disappears, auditor should take appropriate note.

[25] Different CAS' have different ways to trigger covert FP. In most of the cases the covert FP flashes appear on the screen for very less duration say milliseconds, therefore the Auditor is not able to capture the same. In that case a screen shot of the provisioning whether in SMS or CAS or logs should be taken and considered as a proof and enclosed with the audit report.

S. no	Regulatory Provision	Audit Procedure
4	**Schedule III – D 4** The fingerprinting should not be removable by pressing any key on the remote of STB.	a) Auditor should trigger a fingerprint of at least 120 seconds or above duration from SMS/CAS to the test STB. b) While fingerprint is displayed on STB output connected to TV screen, auditor should press every key on the STB remote control and STB front panel. c) Auditor should confirm that no action while pressing buttons on remote or on STB box (soft boot or hard boot) makes the displayed fingerprint disappear even momentarily for the whole duration of FP. d) If fingerprint disappears with any key action, this requirement is not complied with. e) If may be noted that in case if FP more than 60 seconds is not triggered through SMS/CAS then multiple commands or repetitions of such FPs may be sent to confirm the compliance.
5	**Schedule III – D 5** The finger printing should be on the top most layer of the video.	
6	**Schedule III – D 6** The finger printing should be such that it can identify the unique STB number or the unique VC number.	Auditor should trigger fingerprint on two test STBs and confirm the fingerprint displayed are unique to the VCs in the STBs (UA no. in card-less STBs).
7	**Schedule III – D 7** The fingerprinting should appear on the screens in all scenarios, such as menu, Electronic Program Guide (EPG), Settings,	a) Auditor should trigger 120 seconds or more duration fingerprint on test STB and use remote control of STB to navigate to Menu page, EPG page, Settings page, Blank screen and Games page. b) Fingerprint should be displayed on all the above-mentioned pages.

S. no	Regulatory Provision	Audit Procedure
	blank screen, and games etc.	
8	**<u>Schedule III – D 8</u>** The location, font color and background color of fingerprint should be changeable from head end and should be random on the viewing device.	Auditor should trigger fingerprint on test STB multiple times, each time with at least 3 different permutation/combinations of location, font color, and background box color. The locations of the fingerprint should be seen on random areas of the TV screen to make it unpredictable to viewer.
9	**<u>Schedule III – D 9</u>** The finger printing should be able to give the numbers of characters as to identify the unique STB and/or the VC.	Auditor should trigger fingerprint on two test STBs and confirm the fingerprint displayed are corresponding uniquely to the actual VCs in the STBs (UA no. in cardless STBs).
10	**<u>Schedule III – D 10</u>** The finger printing should be possible on global as well as on the individual STB basis.	a) Auditor should trigger fingerprint to all STBs and confirm fingerprints are displayed on all test STBs provided DPO has no objection while testing the feature of global FP on all its STBs. b) If DPO has objection then this feature can be checked by giving ECM FP on a non-popular channel. c) Auditor should trigger fingerprint to one test STB and confirm it is displayed on the particular STB only.
11	**<u>Schedule III – D 11</u>** The overt fingerprinting should be displayed	a) Auditor should obtain fingerprint Schedules from some (minimum 2 broadcasters)[26] broadcaster channels distributed by the DPO.

[26] There are many broadcasters and it would not be possible to check this requirement for every broadcaster. Therefore, validating this requirement for minimum two broadcasters will suffice the requirement.

S. no	Regulatory Provision	Audit Procedure
	by the distributor of television channels without any alteration with regard to the time, location, duration and frequency.	b) Auditor should trigger fingerprinting on those channels where the broadcaster fingerprinting is running on regular interval and take screenshot of broadcaster fingerprint along with DPOs fingerprinting seen on TV screen as proof of compliance[27].
12	**Schedule III – D 12** Scroll messaging should be only available in the lower part of the screen.	a) Auditor should trigger scroll message of 120 characters from the DPO's SMS or CAS targeted to all test STBs. b) The scroll should be displayed as a horizontally moving ticker on the lower part of the TV screen.
13	**Schedule III – D 13** The STB should have a provision that fingerprinting is never disabled.	a) Auditor should trigger a fingerprint of 120 seconds or more duration FP from SMS/ CAS to the test STB. b) The STB should be rebooted, and fingerprint should reappear again automatically. If fingerprint disappears, this requirement is not complied with. c) The STB declaration **(Annexure 4)** should also mention this capability.
14	**Schedule III – D 14** The watermarking network logo for all pay channels shall be inserted at encoder end only. Provided that only the encoders deployed after coming into effect of the Amendment	To confirm that the encoders support watermarking network logo insertion: a) Auditor should disconnect all test STBs from RF signal and then observe the TV screen. b) If network logo is still visible on TV screen, then the requirement of insertion of network logo at the encoder end is not complied with. c) Screenshot of the observations should be included as part of the audit report.

[27] This is to check that broadcaster fingerprinting and DPO fingerprinting should not interfere with each other while appearing on the screen simultaneously. This is to avoid only broadcaster fingerprinting being checked.

S. no	Regulatory Provision	Audit Procedure
	regulations shall support watermarking network logo for all pay channels at the encoder end.	***Note:*** Only the encoders deployed after coming into effect of the Amendment regulations shall support watermarking network logo for all pay channels at the encoder end. The above requirement of schedule III can be checked and verified by auditor only if the DPO has deployed encoders with watermarking network logo capability. If the DPO encoders are old (procured before 30th October 2019) and do not have this capability the same observation should be– captured in the audit report along with declaration of DPO mentioning the deployment of encoders before 30th October 2019[28]. In case of infrastructure sharing, the infrastructure provider shall insert network logo watermarking from the encoder end. The infrastructure sharing seeker should provide logo through STB/middleware.[29]

(C) Set Top Box (STB):

S. no	Regulatory Provision	Audit Procedure
1	**<u>Schedule III – E1</u>** All STBs should have a Conditional Access System.	To inspect all models of STBs available in the inventory of MSOs or deployed (2 units of each make & model) under test and confirm the STB serial no./VC no./UA no. exists in the live CAS database.
2	**<u>Schedule III – E 2</u>** The STB should be capable of decrypting the Conditional Access messages	The auditor will check and verify whether the STB is able to execute all the commands whether activation/de-activation of particular channel or package or

[28] The encoders deployed before 2019 generally do not have this capability. Further, replacing encoders is a costly affair and will have financial implications on DPOs. These old encoders will be phased out eventually with new encoders.

[29] In accordance with Telecommunication (Broadcasting and Cable) Services Interconnection (Addressable Systems) (Seventh Amendment) Regulations, 2026 (1 of 2026) [hereinafter called Seventh Amendment Regulations 2026], clause has been amended.

Watermarking insertion through encoders is an essential feature to be used in case of piracy detection as explained in para 170 and 172 of explanatory Memorandum of above Seventh Amendment Regulations 2026.

S. no	Regulatory Provision	Audit Procedure
	inserted by the Head-end.	FP/messaging command without any major delay or issue.
3	**<u>Schedule III – E 3</u>** The STB should be capable of doing fingerprinting. The STB should support both Entitlement Control Message (ECM) and Entitlement Management Message (EMM) based fingerprinting.	a) To trigger fingerprinting on a particular channel and confirm fingerprint is seen on all test STBs on that particular channel only at the same time. This is ECM based fingerprinting. b) To trigger fingerprinting on all channels and confirm fingerprint is seen on all test STBs on all channels at the same time. This is EMM based fingerprinting. c) The auditor will check and verify both types of fingerprinting on each and every model of STB available with DPO in its inventory.
4	**<u>Schedule III – E 4</u>** The STB should be individually addressable from the Head-end.	The auditor will verify whether the STB are addressable by performing simulation tests on the STB for activation/de-activation.
5	**<u>Schedule III – E 5</u>** The STB should be able to receive messages from the Head-end.	a) Auditor should trigger scroll message of 120 characters from the DPO's SMS targeted to all test STBs. b) The scroll should be displayed in its entirety as a horizontal moving ticker on the lower part of the TV screen.
6	**<u>Schedule III – E 6</u>** The messaging character length should be minimal 120 characters.	a) Auditor should trigger scroll message of 120 characters from the DPO's SMS/CAS[30] targeted to all test STBs.

[30] Some CA systems do not allow to integrate API's for certain features with other system (SMS) because of their security concerns, therefore this feature can also be checked for compliance directly through CAS. Therefore, the word 'CAS' is added in the above-mentioned clause. Scroll message can be triggered either from CAS or from SMS since the end objective is that scroll message should be minimum of 120 characters which can be achieved both with CAS and SMS, therefore this flexibility is allowed.

S. no	Regulatory Provision	Audit Procedure
		b) The scroll should be displayed in its entirety as a horizontal moving ticker on the lower part of the TV screen.
7	**Schedule III – E 7** There should be provision for global messaging, group messaging and the individual STB messaging	a) Auditor should trigger scroll to all STBs and confirm it is displayed on all test STBs. b) Auditor should trigger scroll to one test STB and confirm it is displayed on the particular STB only.
8	**Schedule III – E 8** The STB should have forced messaging capability including forced finger printing display.	Auditor should trigger Forced message (scroll message/or any other message which cannot be disabled by any intervention in its command duration) and Fingerprinting from SMS or CAS to test STBs to confirm availability of Forced messaging and fingerprinting commands. It means, when a forced messaging/FP is run on the STB, no buttons on the remote should function which can disable the force message or Fingerprinting. Further, the FP command should appear as per parameters given through SMS/CAS. Screenshots may accordingly be enclosed.[31]
9	**Schedule III – E 9** The STB must be compliant to the applicable Bureau of Indian Standards	a) Auditor should take copies of BIS certificates from the DPO for each make & model of STB procured after 29th December 2018. The BIS certificate of a STB may be of the year when the STB was purchased. Alternately, Auditor may also verify the validity of the BIS Certificates online (by inputting the Registration Number of the first BIS Certification of the respective STB Models). Screenshots of the online

[31] The earlier audit procedure was not practical as it was asking both fingerprint and message through scroll message which was not feasible. Majority of the auditors gets confused with the word forced message because they think it is the forced message which covers the entire viewer screen and therefore insist on this requirement during audit process. This type of forced messaging is redundant and is not used anymore. Further, any message is a forced message which does not gets disabled through any means till its-duration. A scroll message is also a type of forced message if it appears till its duration and does not get disabled.

S. no	Regulatory Provision	Audit Procedure
		verification of such BIS validity should be provided in the Audit Report. b) The certificates should mention exact STB make & model nos. c) As of the audit date, the certificates should be valid for the STB models which are available in the physical stock and the current inventory of DPO for deployment.[32] For old STB models deployed before 29th December 2018, the DPO needs to have at least one BIS Certification (whether valid/expired) to prove BIS Compliance at the time of seeding the STBs.[33]
10	**<u>Schedule III – E 10</u>** The STBs should be addressable over the air to facilitate OTA software upgrade.	Auditor should ensure this capability is mentioned in STB vendor certificate **(Annexure 4).[34]**
11	**<u>Schedule III – E 11</u>** The STBs with facilities for recording the programs shall have a copy protection system	Auditor to check and report: a) For STBs having recording facility to internal and/or external storage devices such as USB/Hard Disk drives, auditor should check recorded content plays only on the specific STB where content was recorded. b) Auditor to check that scheduled fingerprint and scroll messaging is

[32] It is difficult for DPOs to submit the valid BIS certificates for STBs which are not part of their inventory because of two reasons. First, most of the old STB models are discontinued by the vendor and second, sometimes DPOs do not have existing business relationship with the STB vendors. This amendment will help to mitigate this issue.

[33] 2017 is changed to 29th December 2018 because the implementation date of Interconnection Regulation 2017 is 29th December 2018.

[34] The STB vendor can only certify that its STBs support OTA software up gradation facility. Further, the Auditor cannot check this feature on test STBs until or unless any OTA software up-gradation is pending or scheduled by DPO during audit visits, because it is a major exercise and carried out in exceptional cases. Therefore, the STB vendor declaration w.r.t. this feature is good enough.

S. no	Regulatory Provision	Audit Procedure
		displayed even when stored content is played on the STB. c) Auditor should confirm that recorded content cannot be played if STB is in de-active state.

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 CAS architecture). For DPO, with multiple Headends and additional CAS/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.[35] 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 TS recording and ground VC are also required the auditor may take additional one week for sample verification of the recordings and ground VC 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.[36]

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 days[37] 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

[35] It has been brought to the notice of TRAI that the existing audit guidelines for audit completion are very stringent and it is difficult to complete this audit within the stipulated timeframe. Further, the audit manual should provide timelines for overall completion of audit and should not control the audit timelines on micro level.

[36] It has been brought to the notice of TRAI that verification and analysis of TS recording and ground VCs is a time consuming activity and requires additional time.

[37] As per Seventh Amendment Regulations 2026.

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 shall include the Audit to validate compliance with the Schedule III of the Interconnection Regulations 2017 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 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 CAS and SMS 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 CAS 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 CAS. The auditors will then check the SMS and CAS logs also regarding command execution timings to validate the integration between CAS and SMS.

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

i. ***Extraction of as on date data dumps from the SMS and CAS server deployed by DPO for SMS and CAS data reconciliation[38].***

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[39].

iii. ***Analysis on data dumps to verify ~~the~~ as on date active[40]count of STBs available on the network of DPO.***

iv. ***Analysis on data dump to report the active STB 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 details (both from SMS & CAS 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.[41]***

vi. ***Verification and reporting of Channel to package mapping along with service ID (with creation, modification and discontinue date) from SMS & CAS on the minimum 20% random selected dates of the audit period (as per point ii above).[42]***

[38] The above amendments will clarify the reason for the extraction of as on date data dumps.

[39] The suggested modification will bring even sample size selection in the audit period. The amended clause will also ensure audit efficacy.
If the variance in MSR of a particular broadcaster is more than 1%, then the MSR verification needs to be carried out for entire audit period. This will ensure audit efficacy in MSR verification process.

[40] 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 CAS.

[41] The amendment regarding highlighting 15% variance will result in highlighting those DPOs who have more than 15% variance in its CAS and SMS data.

[42] Random 20% sample assessment is good for the audit period of 12 months.

vii. ***Reconciliation of complete VC and STB data from CAS and SMS as on date of audit. Any discrepancy of VC not active in SMS but found active in CAS, excluding test/monitoring VC/STB, 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 should be separately recorded.

10.6 Auditor will ensure that no parallel SMS or CAS 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 Audit will check the transaction logs of the audit period to ensure no manipulation in the logs of CAS and SMS are done by DPO to under report the active STB count.

10.8 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.[43]

10.9 The Auditor shall connect the Set-Top Box (STB) 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.[44]

10.10 Analysis and verification of TS recording/VC samples 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.

10.11 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

[43] To identify all mismatches related to LCN and genre during the audit exercise.

[44] For bringing clarity related to reconciliation of genre and LCN offered by DPO.

infrastructure sharing arrangements from the infrastructure provider[45].

- 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 CAS/SMS or both.

In the case of sharing of CAS/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.

11.2 Block schematic diagram of Headend including CAS and SMS.

11.3 Certificate from all the CAS vendors **(Format as in Annexure 1).**

11.4 Certificate from SMS vendors **(Format as in Annexure 2).**

11.5 Signed and stamped copy of subscription audit form as per **Annexure 5**.

11.6 **Monthly SMS report regarding state wise active[46] STB count for the audit period. This report is applicable for all DPOs who have operations in different states.[47]**

[45] 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 CAS, SMS, 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.

[46] 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 CAS.

[47] This will bring more clarity in the above clause that it is only required when DPO have operations in multiple States.

11.7 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.[48]

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.

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.**

[48] 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.

12.9 The data extraction procedure from CAS and SMS should be carried out as mentioned in section 16 of the Audit Manual.

12.10 In case of DPO having multiple Headends, 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 CAS) and submit the report within six weeks. For DPO, with multiple Headends and additional CAS/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[49].

b) In case where verification and analysis of TS recording and ground VC are also required the auditor may take additional one week for sample verification of the recordings and ground VC 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 days[50] 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 CAS) and submission of report

[49] It has been brought to the notice of TRAI that the existing audit guidelines for audit completion are very stringent and it is difficult to complete this audit within the stipulated timeframe.

[50] As per Seventh Amendment Regulations 2026.

within eight weeks. For DPO, with multiple Headends and additional CAS/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 CAS & SMS servers and depute a resource who has complete knowledge of the systems (CAS and SMS). The resource can be common or different for CAS 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 (CAS and SMS) of DPO without his/her permission and assistance.

16.4 If the data extraction from the live SMS and CAS 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 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 CAS and SMS server should be extracted in such a manner that no active STB/VC is left out from the database. The Auditors should acquaint themselves with the data extraction queries that are run on the live CAS & 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 CAS & SMS data. Auditor to certify that the data extraction has been done under his/her supervision.

17. Analysis and Verification of TS recordings/VC samples

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 auditor[51].

17.2 The broadcasters may provide the TS recordings or ground VC (if any) to auditors for verification and analysis of the TS recordings and VC 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 TS recordings or VC samples (if any) with the audit agency.

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

[51] As per Seventh Amendment Regulations 2026.

- The broadcaster cannot share more than 5 TS recordings and 100 VC 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 TS/VC recordings. Broadcaster should ensure that these TS recordings and VC samples are correct and should be provided with date, time and complete address/location details.

- The auditor should verify these TS recordings and VC samples during conduct of audit. In case he/she is not able to find some VC samples in the CAS and SMS database of DPO and TS recordings parameters also have some variation w.r.t TS recordings of headend, then random physical verification of such VC samples and TS recordings also should be carried out by auditor in order to validate the shared VC samples/recordings.

- In such cases where a certain amount of VC samples provided by broadcasters are not found in the CAS and SMS database of DPO then auditor will select minimum five (5) number of VC samples from these VC samples and one (1) TS recordings on random basis for carrying out physical verification to ensure the correctness of samples.

- The cost of carrying out minimum physical verification of these TS recordings and VC 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 6 minimum (5 VC samples and 1 TS) physical inspection needs to be carried out by auditor to validate the TS recordings and VC 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 TS recording and ground samples whenever validation of such VC samples and TS recordings 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 CAS and SMS for minimum 2 years from the date of conduct of audit.

4) It is the responsibility of DPO having shared CAS and SMS systems with its JV companies to share the complete data from SMS and CAS 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.[52]

6) The DPO will share the relevant part of the report, including all annexures[53], 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

[52] As per Seventh Amendment Regulations 2026.
[53] As per Seventh Amendment Regulations 2026.

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 CAS, SMS and other related systems 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 CAS
   d. Change in the CAS version w.r.t last audited CAS
   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 CAS, SMS servers and related addressable system to the auditor and depute a resource/expert of deployed CAS 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 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.[54] The DPO should also allow broadcaster's representative in case of audit initiated by Broadcaster's 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.[55] 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 TS recordings and 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

[54] As per Seventh Amendment Regulations 2026.

[55] 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.

fingerprint schedule, assistance in physical verification of sample TS recordings/ground VC 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 direct or influence, in any manner, the conduct of the audit[56]. 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 two 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 TS recordings and ground VC samples are provided by broadcasters then auditor should verify whether these TS recordings reconcile with headend TS recordings and VC samples are also available in the CAS and SMS database of DPO.

5) If the TS recordings parameters are different from those recorded at headend and shared VC samples are not found in the CAS and SMS system of DPO then auditor will also carry out the physical

[56] As per Seventh Amendment Regulations 2026.

verification of minimum 5 VC samples and 1 TS recordings to check the authenticity of same. These 6 samples (5 VC and 1 TS) shall be selected on random basis from the list of samples/TS which were not found in the system of DPO.

6) **The audit period shall be as specified in the Interconnection Regulations 2017[57].**

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, CAS 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 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 CAS systems as mandated in Schedule III 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.

[57] As per Seventh Amendment Regulations 2026.

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 empaneled 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 expense~~s~~.

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 data[58] 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.

[58] 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.

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 Management Studio & SQL Server Data Tools (SSDT)	Microsoft SQL Server developer edition	Microsoft SQL Server developer edition	Microsoft SQL Server developer edition/Microsoft Access	Microsoft SQL Server Express/ 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 CAS Vendor

(On CAS company letterhead)

TO WHOMSOEVER IT MAY CONCERN

This is to certify that M/s __________(DPO Name)______________________________address:____________________________ ______________________________

having its DAS headend at ____

has installed Conditional Access System (CAS) from our company for its distribution network.

Date of CAS Installation and operational: ________ CAS Version: __________

CAS ID: _________________, Network ID: _________________________

Location and number of CAS servers (Database server, ECMG, EMMG): __________________

Details of main and back up CAS servers installed:_______________-- _________

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

No. of ECMG and EMMG server -

Location of ECMG and EMMG servers

Number of DPOs/networks configured (applicable in case of infrastructure sharing)[59]

Server time format:________________________________

Database detail:_________________________________

Attached schematic diagram of CAS network including ECMG/EMMG & other servers 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).[60]

With respect to the CAS installed at above mentioned headend and in terms of Schedule-III of THE TELECOMMUNICATION (BROADCASTING AND CABLE) SERVICES INTERCONNECTION (ADDRESSABLE SYSTEMS) REGULATIONS, 2017 (as amended) of TRAI, we confirm the following:

[59] The above modification in this annexure is made keeping in view the provisions of sharing infrastructure.

[60] The above modification in this annexure is made keeping in view the provisions of sharing infrastructure.

1) All activation and deactivation of STBs can be done with the commands of the SMS.

2) The current version of CAS does not have any history of hacking.

3) We have the capability of upgrading ~~of~~ CAS in case it gets hacked.

4) The CAS is currently in use by other pay TV services and it has an aggregate of at least 1 million subscribers in the global pay TV market.

5) It is not possible to alter the data and logs recorded in the CAS.

6) That all the CAS systems provided to the said distributor at all the locations (head-ends) have been duly reported.

7) We, the CAS system provider are able to provide monthly and date wise log of activation and deactivation of a particular channel or of a particular Bouquet/Subscriber Package.

8) This CAS is capable of individually addressing subscribers, on a channel by channel and STB by STB basis.

9) This CAS is independently capable of generating, recording, and maintaining logs, for the period of at least immediate preceding two consecutive years, corresponding to each command executed in the CAS including but not limited to activation and deactivation commands issued by the SMS.

10) The CAS has the capability of upgrading STBs over-the-air (OTA), so that the connected STBs can be upgraded.

11) The CAS has the capacity to activate or deactivate services or STBs of at least 5% of the subscriber base of this customer's distribution network within 24 hours.

12) That we ____________(CAS Company Name) are fully compliant to the requirements of CAS system as per schedule III of THE TELECOMMUNICATION (BROADCASTING AND CABLE) SERVICES INTERCONNECTION (ADDRESSABLE SYSTEMS) REGULATIONS, 2017 (as amended) of TRAI.

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

Thanking you,

For (CAS company name)

(Signature)

Name :

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

Date :

Company seal :

Date: (within 90[61] days prior to audit)

[61] The certificate validity should be amended from 30 days to 90 days because sometimes the audit gets delayed after the issuance of certificate and by the time report is submitted, the CAS certificate issued by vendor gets expired. 90 days' timeline will ensure the certificate validity till the issuance of audit report.

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/spilts and date of creation: __________________________

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

Please find enclosed the schematic diagram of SMS and CAS system(s) integration. And also the Number of DPOs/networks configured (in case infrastructure sharing)___________[62]

With respect to the SMS installed at above mentioned headend and in terms of Schedule-III of THE TELECOMMUNICATION (BROADCASTING AND CABLE) SERVICES INTERCONNECTION (ADDRESSABLE SYSTEMS) REGULATIONS, 2017 (as amended) of TRAI, we confirm the following:

1. The SMS has the capacity to activate or deactivate services or STBs of at least 5% of the subscriber base of the distributor within 24 hours.

[62] To cover the provisions of sharing infrastructure.

2. We have the technical capability in India to be able to maintain our systems on 24x7 basis through the year.

3. We, the SMS system provider are able to provide monthly and date wise log of activation and deactivation on particular channel or on a particular Bouquet/Subscriber Package with date/time stamp.

4. The SMS is capable of individually addressing subscribers, on a channel by channel and STB by STB basis.

5. This SMS is independently capable of generating log of all activations and deactivations.

6. The SMS is independently capable of generating, recording, and maintaining logs, for the period of at least immediate preceding two consecutive years, corresponding to each command executed in the SMS including but not limited to activation and deactivation commands (as per period of service).

7. Please find enclosed sample log of activations & deactivations of a channel generated from this SMS system.

8. That we ___________(SMS Company Name) are fully compliant to the requirements of SMS system as per schedule III of the of THE TELECOMMUNICATION (BROADCASTING AND CABLE) SERVICES INTERCONNECTION (ADDRESSABLE SYSTEMS) REGULATIONS, 2017 (as amended) of TRAI.

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)/Authoirzed 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.)[63]

Type of DPO: CATV/HITS/IPTV/DTH
.... Date : ....

Address of the headend ....

Headend technical person : ....Contact No. ..

1	No..of SD & HD Channels presently running in the network		**FTA**	**PAY**	**TOTAL**	**Total no. of Transport Stream**
		SD				
		HD				
Sl. No.	**CAS Make**	**Version**	**For Software based (Cardless)**			**Server Location**
			Encryption Strength	**Key Length**	**Video Scrambling**	
1						
2						
Sl. No.	**SMS Make**	**Version**	**Date of Installation**		**Server Location**	
1						
2						
Sl. No.	**STB Make**	**Model**	**(HD, SD, PVR)**	**MPEG 2/4**	**Card/ Cardless**	**Embedded CAS Name**
1						
2						
3						
4						
5						
A) Conditional Access System (CAS) & 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					

[63] Keeping in view of the provisions of sharing infrastructure the above amendments are made.

	b. Subscription Contract number		
	c. Name of the subscriber		
	d. Billing Address		
	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 CA integrated for activation and deactivation process from SMS to be simultaneously done through both the systems? Is the CA system independently capable of generating log of all activation and deactivations?		
4	Are SMS & CAS capable of individually addressing subscribers, on a channel by channel and STB by STB basis?	**CAS**	**SMS**
5	For VC based CAS, is the STB & VC paired from head-end to ensure security?		
6	Is CAS 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 CAS & 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 cannot be redeployed?	**CAS**		**SMS**		
9	Is CAS able to provide reports at any desired time about:					
	a. Active and De-active VC wise details as on any particular date					
	b. STB-VC Pairing / De-Pairing c. STB Activation / De-activation d. Channels Assignment to STB e. Report of the activations or the deactivations of a particular channel for a given period.					
10	Is CAS & SMS able to provide reports at any desired time about:	**CAS**		**SMS**		
	a. VC wise log of changes in packages/channels for any particular period					
	b. Logs of creation and modification of packages for any particular period					
12	Total No. of STBs deployed in the network presently?	In field SD: In field HD:				
B) Fingerprinting & Scroll messaging		**STB1**	**STB2**	**STB3**	**STB4**	**STB5**
		Yes/No				
1	Is FP Facility available (ECM/EMM) 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?					
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 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 STB capable of doing finger printing and support Entitlement					

	control message (ECM) based finger printing?					
	Is the STB capable of doing finger printing and support Entitlement management Message (EMM) based finger printing?					
11	Is the scroll messaging character length 120 or more?					
12	Does STB has forced messaging capability?					
13	Is there provision for the global messaging, group messaging and the individual STB messaging?					
D) STB		**STB1**	**STB2**	**STB3**	**STB4**	**STB5**
		Yes/No				
1	Is Valid BIS certificate of each model of STB available?					
2	Does the STBs with facilities for recording the programs have copy protection system?					
3	Is STB addressable to be upgraded by OTA?					
4	Watermark of the network logo is Encoder or STB generated?					

I __(_name)______ undertake that the information provided above is true and full disclosure of all the CAS and SMS system(s) and STB 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)/Authorized signatory

Company seal :

Annexure 4

Format of declaration from STB Vendor

(On STB company letterhead)

TO WHOMSOEVER IT MAY CONCERN

This is to certify that M/s __________(DPO Name)______________________________address:____________________________ ______________________________

having its DAS 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-III of THE TELECOMMUNICATION (BROADCASTING AND CABLE) SERVICES INTERCONNECTION (ADDRESSABLE SYSTEMS) REGULATIONS, 2017 (as amended) of TRAI w.r.t STB requirements as mentioned below:

1. All STBs should have a Conditional Access System
2. The STB should be capable of decrypting the Conditional Access messages inserted by the Head-end.
3. The STB should be capable of doing fingerprinting. The STB should support both Entitlement Control Message (ECM) and Entitlement Management Message (EMM) based fingerprinting.
4. The STB should be individually addressable from the Head-end.
5. The STB should be able to receive messages from the 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 STB should have forced messaging capability including forced finger printing display.
9. The STB must be compliant to the applicable Bureau of Indian Standards.
10. The STBs should be addressable over the air to facilitate OTA software upgrade.
11. The STBs with facilities for recording the programs shall have a copy protection system

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 subscription audit form

(Letter head of DPO)

(In the case of infrastructure sharing separate Subscription Audit Form shall be filled by each of the Infrastructure Seeker also)[64]

S.No	Area	Data requested	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		Transport streams:	
3.5		Number of Transport Streams	
3.6		Watermarking:	
3.7		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 CAS	
4.3		STB-VC ID Pairing details if applicable	
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 wise, Group/All)	
4.8		Messaging (STB 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	

[64] Keeping in view of the provisions of sharing infrastructure the above amendments are made.

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	**Conditional Access System (CAS)**	**Features**	
6.1		Number of CA systems installed at the headend & the version of each	
6.2		Number of channels configured on each CAS	
6.3		Channel(SID) to package/product mapping	
6.4		Fingerprinting (STB wise, Group/All)	
6.5		Messaging (STB wise, Group/All)	
6.6		Audit/trail/log of all changes for each CAS	
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 status as per the system	
7.3		Activation and deactivation log for each STB/ VC Id	
7.4		Activation and deactivation log of channels and packages for each STB/ VC ID	

Undertaking

I __(_name)______ undertake that the information provided above is true, full and complete disclosure of all the CAS and SMS system(s) and STB has been made above and no information has been concealed.

(Signature)

Name :

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

Company seal :

Annexure 6

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

Contents

(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 Procession*
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 CAS(s)

[

Details of the CAS(s) installed

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

Details of Infrastructure Seekers in case of infrastructure sharing[65]

]

Details of SMS(s)

[

Details of the SMS(s) installed

Detail of the SMS(s) installed with the respective CAS(s)

Details of Infrastructure Seekers in case of infrastructure sharing[66]

]

[65] Amendment made in view of the provisions related to sharing of infrastructure.

[66] Amendment made in view of the provisions related to sharing of infrastructure.

Detail of the Signal Processing Systems

[

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

i. EMM Servers
ii. ECM Servers
iii. Scramblers
iv. QAM
v. Multiplexers
vi. PSI/ SI servers
vii. Fiber transmitters

]

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) as on date[67] *of audit*

[67] In 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 CAS.

ii. Package-wise list and detail of services configured in CAS(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 sharing[68]

]

Set Top Box Management Process

[

Detail of the STB management system w.r.t. following:

i. Authorization process of STB/ VC in CAS,
ii. Transfer of STBs/VCs from DPO to LCO and LCO to consumer

Annexure: Flow Chart of the STB Management

]

Consumer Acquisition Process

[

[68] Amendment made in view of the provisions related to sharing of infrastructure.

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

Annexure: Flow Chart of the Consumer Acquisition Process

]

Data Management Process

[

Explanation of the system and procedure adopted by DPO for management of the data from CAS 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 III COMPLIANCE REPORT

[]

Compliance Report for CAS & SMS

[

Section will cover point-wise compliance for the requirements w.r.t. CAS & SMS specified in the Schedule-III of the Interconnection Regulations 2017

(Ideally in tabular form)

]

Compliance Report for Finger Printing

[

Section will cover point-wise compliance for the requirements w.r.t. fingerprinting specified in the Schedule-III of the Interconnection Regulations 2017

(Ideally in tabular form)

]

Compliance Report for STB

[

Section will cover point-wise compliance for the requirements w.r.t. STB specified in the Schedule-III of the Interconnection Regulations 2017

(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	
MUX configuration to validate number of Transport Streams ("TS")	
Details of QAM installed in the network	
Record of PSI/ SI servers (for EPG and LCN)	
Watermarking provisions	
Encryption status of the channels/ services	
Compliance Status of the CAS & SMS	
Compliance Status of the Fingerprinting	
Compliance Status of the STBs deployed	
Analysis of TS / VCs	

]

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

]

a)

b) Format of Subscription Audit Report (**Annexure 7**).

Annexure-7

Audit Report of verification carried out for

conforming the completeness, truthfulness and correctness of

Monthly Subscription Reports (MSR) submitted to

<Name of the Broadcaster> by

M/s _______________

Contents

(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 Procession*
- *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 CAS(s)

[

Details of the CAS(s) installed

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

]

Details of SMS(s)

[

Details of the SMS(s) installed

Detail of the SMS(s) installed with the respective CAS(s)

]

Detail of the Signal Processing Systems

[

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

i. EMM Servers
ii. ECM Servers
iii. Scramblers
iv. QAM
v. Multiplexers
vi. PSI/ SI servers
vii. Fiber transmitters

]

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 verification*[69].

[69] 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 CAS.

ii. *Package-wise list and detail of services configured in CAS(s) for minimum 20% random selected dates of MSR verification.*[70]

]

Network Architecture

[

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

]

Set Top Box Management Process

[

Detail of the STB management system w.r.t. following:

i. *Authorization process of STB/ VC in CAS,*
ii. *Transfer of STBs/VCs from DPO to LCO and LCO to consumer*

Annexure: Flow Chart of the STB Management

]

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

[70] 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 CAS.

Identification process of each STB in cases when multiple STB are assigned to single consumer

Annexure: Flow Chart of the Consumer Acquisition Process

]

Data Management Process

[

Explanation of the system and procedure adopted by DPO for management of the data from CAS 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)

]

[]

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 CAS	**As per SMS**	**Present in SMS not in CAS**	**Present in CAS not in SMS**
Active count[71]				
CAS 1				
CAS 2				
CAS 3				

CAS N				

[71] Any reconciliation or audit needs to be carried on the active count of SMS and CAS to get the true picture of the system. It is difficult to ascertain de-active count from CAS as its primary function is to encrypt the data. Majority of the standard CAS do not provide this de-active count data therefore de-active reconciliation is complex exercise and may vary from CAS to CAS. Therefore, all reconciliation needs to be carried out on active count of SMS and CAS.

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 CAS architecture, or in case a DPO has multiple CAS, 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 CAS i.e. In case of sharing CAS(s) or in case a DPO has multiple CAS, the data can be reconciled in totality or by summing up the package/channel wise count from CAS and reconciling the same with SMS count.[72]

[72] Under the existing audit guidelines, reconciliation of CAS and SMS needs to be carried out channel vs channel and package vs package (linear reconciliation). This requirement is difficult to meet in cases where DPO have many packages or where CAS is shared between different JV entities because in CAS there is a limitation of packages to be formed. Thus, it is not possible to segregate package/channel wise data in CAS w.r.t packages/channel formed in SMS and carry linear reconciliation however reconciliation of total CAS package/channel vs total SMS package/channel may be carried out in such cases. Therefore, alternate reconciliation methods in such cases are also allowed.

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 CAS 1	As per CAS 2	- - - - - - As per CAS N	Total CAS	As per SMS	Reported MSR Count to Broadcasters	Variance (CAS-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								
DPO’s Package 1 Subscriptions								
DPO’s Package 2 Subscriptions								
- - - - - - -								
DPO’s Package N Subscriptions								

[

Section will cover reports for at least 12 weeks i.e. 12 dates for all the PAY Channels

]

Deviation in the count

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***
Observations on the Data Extraction Process	
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 Completeness, Correctness and Truthfulness of the Subscriber count

]

ANNEXURES OF SUBSCRIPTION AUDIT REPORT

[

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

]

Annexure-8

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 CAS……………………………..

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**	**MIB Registration No of Infrastructure seeker**	**Remark**
		Headend Type (CATV/DTH/HITS /IPTV)	**Location**	**Address**			

Details of Infrastructure seeker(s) sharing CAS							
S.No	**CAS Name**	**Details of CAS being shared**			**Name of the Infrastructure seeker**	**MIB Registration No of Infrastructure seeker**	**Remark**
		CAS Version	**CAS Make**	**Address**			

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

						Infrastructure seeker	

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