भारत सरकार
प्रधान मुख्य आयकर आयुक्त का कार्यालय,
10 वी मंजिल, सी ब्लॉक, आयकर शिखर,
10-2-3,ए.सी. गार्ड्स, हैदराबाद-500 004
टेलीफोन: 040-23236281

GOVERNMENT OF INDIA
Office of the Pr. Chief Commissioner of Income Tax,
10th Floor, C Block, Income tax Towers,
10-2-3, AC Guards, Hyderabad-500004
Tel No:040-23236281
Email:hyderabad.cit.admin.tps@incometax.gov.in

F. No. 01/CIT (Admn & TPS) /Dept Exams/2026-27 **Date:12.08.2026.**

OFFICE MEMORANDUM

To
All candidates appearing for the I.T. Departmental Examination–2026 in the Pr. CCIT Andhra Pradesh & Telangana Region.

Subject: Departmental Examination–2026, Circulation of "Compendium on IT Applications and Operations" – Study material for the paper "IT Applications & Operations" of Departmental Examination–2026 – Reg.

Attention of all candidates appearing for the Departmental Examination–2026 in the Andhra Pradesh & Telangana Region is invited to the Compendium on IT Applications and Operations circulated by the Directorate of Human Resource Development (Examination Division), CBDT, vide F. No. HRD/Exam/2026-27/354 dated 11.08.2026.

2. The said Compendium has been prepared as study material for the paper "IT Applications & Operations" for the following cadres:

i. Income Tax Officers – Paper-V
ii. Income Tax Inspectors – Paper-IV
iii. Ministerial Staff – Paper-IV

3. The Compendium comprises 18 chapters covering the combined prescribed syllabus for the above three cadres. Candidates are advised to study only those portions relevant to their respective cadre, as indicated under the "Applicable to" marking at the beginning of each chapter.

4. The Compendium is intended as a self-study aid for preparation for the Departmental Examination–2026. It is not an exhaustive statement of the law or a substitute for the bare Act, Rules, official ITBA instructions and relevant CBDT Circulars/Notifications, which shall prevail in case of any conflict.

5. All candidates concerned are, therefore, requested to make use of the Compendium and study the relevant portions applicable to their respective examination paper/cadre for effective preparation for the Departmental Examination–2026.

6. The Compendium has also been made available on the official website of the Income Tax Department, Hyderabad, for easy access by all concerned. Candidates are advised to make use of the study material and share its availability with their fellow candidates to ensure wider dissemination.

7. All concerned are requested to give wide publicity to the availability of the Compendium through the departmental website and notice boards and make full use of the study material for preparation for the Departmental Examination–2026. This is in line with the request of the Directorate of HRD, Examination Division, New Delhi for wide dissemination of the Compendium among eligible candidates.

8. The Compendium is circulated for information and necessary action by all concerned.

(TADIMALLA SUNIL GOUTAM, IRS)
Addl.Commissioner of Income Tax(Hqrs) (Admn. & Vig)
O/o Pr. CCIT, AP & TG, Hyderabad

Encl.: Compendium on IT Applications and Operations.

Government of India
Ministry of Finance, Department of Revenue
Central Board of Direct Taxes
Directorate of Human Resource Development
(Examination Division)

5th Floor, Mayur Bhawan, Connaught Place, New Delhi - 110001

F.No. HRD/Exam/2026-27/354 Dated: 11.08.2026

To,

1. All Pr. Chief Commissioners of Income-tax
2. All Pr. Directors General / Directors General of Income-tax
3. Examination In-Charge O/o all Pr. CCsIT

Subject: Compendium on IT Applications and Operations, Study material for the paper "IT Applications & Operations", Departmental Examination, 2026 - Circulation thereof - regarding.

Madam / Sir,

I am directed to forward herewith the Compendium on IT Applications and Operations (enclosed), prepared by the Examination Division, Directorate of HRD, as study material for the paper "IT Applications & Operations" (objective type, without books) of the Departmental Examination–2026, common to the 03 cadres - ITO (Paper-V), ITI (Paper-IV) and Ministerial Staff (Paper-IV).

2. The Compendium comprises 18 chapters covering the combined prescribed syllabus, with the applicable cadres marked at the head of each chapter. Candidates are advised to study only the portions relevant to their own cadre's syllabus, using the "Applicable to" marking.

3. The Compendium is a self-study aid intended to facilitate preparation. It is neither an exhaustive statement of the law nor a substitute for the bare Act, the Rules, the official ITBA instructions and the relevant CBDT circulars and notifications, which shall prevail in case of any conflict.

4. It is requested that the Compendium be given wide publicity among all eligible candidates in your Region/charge, including through the regional websites and notice boards, and that its availability on the departmental webpage be brought to the notice of all concerned. Officers in charge of training institutes (MSTUs/NADT-RC) may also use it as reference material for pre-examination coaching.

5. This issues with the approval of the Chairman, CBDT.

Yours faithfully,

Enclosure: As above

(Smita Verma)
Addl. Director of Income Tax (Exam), HRD

Copy for information to:

1. PPS to Chairman, CBDT for kind information.
2. PPS to Member (Administration), CBDT for kind information.
3. Pr. DGIT (HRD), Delhi for kind information.
4. Pr. DGIT (Training), Delhi for wide circulation in all the training institutes.
5. Web Manager of www.incometaxindia.gov.in — for publishing the Compendium.
6. Guard file.

Addl. Director of Income Tax (Exam), HRD

आयकर विभाग · INCOME TAX DEPARTMENT

Government of India · Central Board of Direct Taxes

COMPENDIUM

IT Applications & Operations

Departmental Examination – 2026

Income Tax Officers (Paper V) · Income Tax Inspectors (Paper IV) · Ministerial Staff (Paper IV)

⚠ DISCLAIMER — FINANCIAL YEAR 2025–26 ONLY

This is a **comprehensive compendium** covering the **combined syllabus of all three cadres** (ITO, ITI and Ministerial Staff). Every reader is requested to **take up and read only the points relevant to their own cadre's syllabus** — refer to the "Applicable to" marking at the head of each chapter.

It is a **study aid** prepared solely for the **Departmental Examination–2026** and reflects the law, rules and departmental systems **as applicable for Financial Year 2025–26 (Assessment Year 2026–27)**. It must be used **only for the examination of the current financial year**. It is **not** a statutory or officially issued publication and must be updated before use in any subsequent examination cycle. In case of any conflict, the bare Act, the Rules, official ITBA instructions and CBDT circulars/notifications shall prevail.

How to use this compendium

This is a self-study reference for serving Income Tax Department employees preparing for the *IT Applications & Operations* paper. It is organised into **18 chapters** across seven parts, covering the prescribed syllabus for all three cadres. Each chapter states the cadres it applies to, the syllabus reference, an educative treatment of the topic (with "what it is / why it matters to the taxpayer and the Department" explainers for key concepts), the **legal & procedural references** (Income-tax Act, 1961 sections/rules and the relevant schemes/notifications), **Key Takeaways** (high-yield consolidating points), and **key terms**.

> **Comprehensive compendium — read what is relevant to you.** This is a **comprehensive** compendium covering the **combined syllabus of all three cadres** (ITO, ITI, MS). Every reader is requested to **take up and study only the points relevant to their own cadre's syllabus** — use the **"Applicable to"** marking at the head of each chapter to identify what applies to you.
>
> **Currency:** The legal position is stated as applicable for FY 2025-26 (Finance Act, 2025 and earlier). The Income-tax Act, 2025 is NOT in force for this examination; the Income-tax Act, 1961 (as amended) applies throughout. **Scope note:** The compendium is specific to the Income Tax Department of India and its systems (ITBA, Insight, TRACES, CPC-ITR/TDS, e-Filing). In case of any conflict, the bare Act, the Rules, the official ITBA instructions and the relevant CBDT circulars and notifications shall prevail.

Table of Contents

Part I — The ITBA Platform & Common Services

01. Introduction to ITBA and the ITD Application Ecosystem

Applicable to: ITO Paper-V, ITI Paper-IV, MS Paper-IV (all three cadres).

Syllabus reference: ITBA Applications Modules — Brief introduction to the ITBA Portal; orientation to the wider Income Tax Department (ITD) application landscape, its login/security model, the worklist-driven way of working, and how the taxpayer-facing and back-office systems fit together.

Overview

Almost every statutory action an Income Tax Department (ITD) officer takes today — allotting a PAN, processing a return, issuing a notice, passing an assessment order, levying a penalty, recovering a demand, disposing of a grievance — is done on one integrated software platform called the **Income Tax Business Application (ITBA)**. This chapter explains, from first principles, **what ITBA is**, why it replaced the old client-server systems, how officers log into it securely over the departmental network, how work reaches an officer through a **worklist**, why every notice/order it produces carries a **Document Identification Number (DIN)**, and how ITBA sits inside a larger family of systems — the taxpayer-facing **e-Filing portal**, the bulk-processing **CPC-ITR**, the TDS system **CPC-TDS/TRACES**, and the analytics platform **Insight**. Because every later chapter builds on these ideas, this chapter is the foundation of the whole paper. The vocabulary introduced here (SSO, RSA token, TAXNET, worklist, work-item, jurisdiction, DIN) recurs throughout the syllabus and warrants careful study.

The two worlds: taxpayer-facing systems vs officer-facing systems

Before naming individual applications, it is useful to fix one organising idea. ITD's software divides into **two worlds**:

- The **taxpayer-facing** world — websites and portals that citizens, businesses, deductors and professionals use from outside the Department (file a return, respond to a notice, download Form 26AS, lodge a grievance). The flagship here is the **e-Filing portal** at www.incometax.gov.in.
- The **officer-facing** (internal) world — the applications departmental staff use from inside the Department to *act* on that data (process the return, raise the notice, pass the order). The flagship here is **ITBA** at itba.incometax.gov.in.

A single taxpayer event usually travels across both worlds:

1. the taxpayer files a return on the e-Filing portal;
2. the return is processed;
3. an officer works the case in ITBA; and
4. the officer's notice appears back to the taxpayer on e-Filing.

Holding this two-world distinction in view makes the remaining elements of the ecosystem straightforward to place.

What ITBA is, and why it replaced the legacy systems

What it is

The **Income Tax Business Application (ITBA)** is ITD's single, integrated, web-based (browser-accessed) platform through which officers and staff carry out their statutory and administrative functions. It is built and run by the **Directorate of Income Tax (Systems)** under the **Pr. DGIT(Systems)** and is accessed at **https://itba.incometax.gov.in** over the departmental network. It is organised into **modules** (PAN, TAN, Assessment, TDS, Rectification, Penalty, Recovery, Appeal, and more), all sitting on a **common, PAN/TAN-centric database** and sharing a common set of services (jurisdiction, worklist, document management, digital signing) supplied by a **Common Functions** module.

Why it matters — to the Department

ITBA lets the Department work in a uniform, workflow-driven, auditable way across the country: the same screens, the same approval routes, the same document trail everywhere. Records follow the PAN rather than being trapped in a local database, cases move automatically on transfer of jurisdiction, and management can monitor pendency and disposal centrally through MIS/dashboards. It also enforces legal safeguards in software — for example, it will not let a notice issue without a DIN, and orders can be digitally signed.

Why it matters — to the taxpayer

For the taxpayer, ITBA is the engine that produces the communications they receive. Because those communications are system-generated and DIN-bearing, the taxpayer can **verify their authenticity** and is protected against spurious or unauthorised notices. Faceless, paperless proceedings — where the taxpayer never needs to visit an office — are possible only because ITBA and the e-Filing portal are integrated with each other.

Why ITBA replaced the legacy AST / ITD application

Before ITBA, officers used a client-server suite generically called the **ITD application**, whose assessment component was the **AST (Assessment Information System)**. The legacy environment had real limitations that ITBA was designed to cure:

- **Isolated databases and no end-to-end workflow.** AST/ITD was largely menu-driven; there was no unified "to-do" list carrying a case from start to finish, and little built-in approval routing.
- **Records tied to a location.** Data did not automatically travel when a case was transferred from one officer to another; manual migration was needed.
- **Weak integration.** It did not talk cleanly to e-Filing or the Centralised Processing Centre, so data was re-keyed and reconciliations were manual.
- **Thin audit trail and no central document repository.** It was hard to reconstruct who did what, and there was no single place for all documents of a PAN.

ITBA answers each of these with a single browser-based application, a **worklist/workflow** engine, PAN-linked records that move on transfer, tight integration with the other systems, a **document management** repository, and a full audit trail.

A primer on the legacy ITD system

What the legacy ITD system was

The **legacy ITD application** was the Department's earlier, pre-ITBA (and pre-faceless) computerised platform, built on a client-server architecture and operated from within departmental offices. Its central component for assessment work was the **AST** — an on-line, menu-driven, parameter-driven module that carried out assessment and related functions: computing tax, calculating interest under the various sections, selecting cases for scrutiny, preparing time-barring lists, and validating due dates and deduction limits. At stations not yet connected to the network, a **Tax Management System (TMS)** ran on standalone computers until those stations were brought on-line. Together, the AST/ITD suite was the software on which assessment orders, demands and related actions were passed before ITBA progressively replaced it.

Why it still matters in FY 2025-26

Although ITBA is now the platform for current work, the legacy ITD/AST system has **not** simply disappeared. It continues to **hold data, records and computations for very old cases** — assessments, demands and case particulars for years that pre-date the migration to ITBA. Officers therefore need a working understanding of how the legacy application operates and, in particular, of where its data resides, because such old cases sometimes still require action today. This arises most often when an old matter is **revived after litigation**: for example, where reassessment proceedings for years such as AY 2015-16 are re-opened following the line of cases culminating in the Bombay High Court's decision in Hexaware Technologies on the validity of s. 148 notices and the JAO/FAO jurisdiction question (the issue is in further appeal as of FY 2025-26). When such a case is revived, the officer may need to retrieve the original computation, order or record from the legacy system in order to give effect to the current proceedings.

A practical consequence worth noting is the treatment of the **DIN** for legacy work: functionality for auto-generation of a DIN was itself enabled inside the ITD/AST application, so a DIN for a legacy ITD/AST order should be generated there and **not** raised separately from the ITBA Common Functions module. Officers processing revived or residual old cases should be alert to which platform actually holds the record and issues the authenticating number.

How ITBA is accessed — network, login and security model

Portal architecture

- **URL:** https://itba.incometax.gov.in. ITBA is *not* on the open internet; it is reachable only from within the departmental network (**TAXNET** nodes) or through the Department's secure remote-access channel (**SSL-VPN**) for field/work-from-home use.
- **Browser + thin client.** Officers use a standard web browser; there is no heavy software to install on each machine, which is what makes nationwide rollout and updates practical.
- **One database, many modules.** All modules read and write a shared PAN/TAN-centric database, so an action in one module (say, an assessment order raising a demand) is visible to another (recovery) without re-entry.

TAXNET — the departmental network

What it is. TAXNET is ITD's private, secure wide-area network (WAN) connecting the Department's offices across India, along with data-centre and connectivity services. ITBA and other internal systems run *over* TAXNET; from outside TAXNET they are not directly reachable. Remote users tunnel in through an **SSL-VPN**.

Why it matters. Because sensitive taxpayer data must never travel over the open internet in the clear, confining the officer-facing systems to TAXNET (plus VPN) is a core **information-security** control. It also gives predictable performance for a very large user base. For the taxpayer, this network isolation is part of why their financial data held by the Department stays protected.

Single Sign-On (SSO)

Single Sign-On (SSO) means the user authenticates **once** and then reaches every ITBA module they are authorised for, without logging in again for each one. Why it matters: it is both a convenience (no repeated logins as an officer moves from PAN work to Assessment to Penalty) and a control (access is granted centrally against the user's role, and can be withdrawn centrally).

The RSA SecurID token and two-factor login

Login to ITBA uses **two-factor authentication**: something the user *knows* (a departmental user-id + password) plus something the user *has* (a personal **RSA SecurID token** that displays a one-time code changing every few seconds). Only the combination lets a user in.

- **What it is:** the RSA token is a small hardware device (or soft-token app) issued individually to the officer that generates a time-based one-time passcode.
- **Why it matters:** a stolen password alone is useless without the physical token, sharply reducing the risk of impersonation and unauthorised access to taxpayer data. This is why tokens must never be shared, and why credentials are sent only to the officer's individual name-based departmental e-mail ID.

The login sequence, home page and dashboard

The login sequence proceeds as follows:

1. the user opens itba.incometax.gov.in over TAXNET (or SSL-VPN);
2. the user enters the departmental user-id and password sent to their official e-mail;
3. the user supplies the current RSA token code; and
4. on success, the user lands on the **ITBA Portal home page** and selects any authorised module from the **Modules** menu (under SSO, with no second login).

After login the officer sees a **home page / dashboard** showing: the pending **Worklist** (work awaiting action), notifications/alerts, MIS and dashboard links, and access to **Online Training on ITBA** (user manuals, help content and FAQs). The dashboard is the officer's principal point of daily interaction with the system.

The worklist model — how work reaches an officer

What a work-item is

A **work-item** is a single unit of pending work — a return to be processed, a rectification application to be decided, a draft order awaiting a Range Head's approval, a grievance to be disposed. Each work-item carries its case history and links to the relevant documents.

What the worklist is

The **Worklist** is the officer's electronic in-tray: the list of all work-items currently sitting with that user for action. Instead of physical files landing on a desk, work "flows" as items into the worklist of whoever holds the relevant jurisdiction and role.

Why the worklist model matters

- **To the Department:** nothing gets lost; every pending action is visible, count-able and monitor-able; approvals route automatically up the hierarchy; and pendency/disposal can be measured through MIS. On transfer of jurisdiction, pending items move with the PAN to the new officer's worklist rather than being stranded.
- **To the taxpayer:** their return, application or response is guaranteed to reach a specific officer's queue and can be tracked, supporting timely and accountable disposal.

How items route — jurisdiction and hierarchy

Work-items route by **jurisdiction** (which PAN/TAN maps to which officer, by area of work, designation and building) and by **hierarchy** (a draft needing approval moves up to the Range Head; a rejected draft moves back down). Related facilities include **Case History / Notings (note sheet)** to see every action taken, **bulk delegation**, and the ability to **seek information** from a subordinate — all recorded in the notings for audit.

The Common Functions module — the shared foundation

What it is

Common Functions is the foundational module that supplies services used by *every* other module rather than doing an assessment or penalty itself. It provides: **jurisdiction** management (the PAN/TAN-to-AO mapping), the

worklist/workflow engine, **Case History/Notings**, **document management**, letter/notice generation, **DSC** (digital signature) handling, **DIN** generation, and the **360° View** of a taxpayer.

Why it matters

Centralising these shared services means every module behaves consistently — the same way to sign, to note, to store a document, to route for approval. It is the reason the whole application operates as a single integrated system rather than as a collection of separate tools.

360° View — the consolidated profile of an assessee

Accessible via **Common Functions → 360° View**, this facility brings together, on a single screen, a comprehensive profile of a taxpayer drawn from across ITBA's modules and the connected systems. Its purpose is to give the officer a complete, rounded picture of the assessee before taking any action, and it is the principal tool for **comparative analysis** of an assessee's data — that is, for viewing the assessee's history and current position side by side rather than opening each module or record separately.

In one consolidated place, the 360° View assembles:

- all **prior assessments and reassessments** passed in the taxpayer's case, across assessment years;
- **appeals filed** by or against the assessee, and their status;
- **refunds issued** to the taxpayer;
- the taxpayer's **income profiles** (returned income and related particulars over the years);
- **demands** outstanding and paid, TDS credits, and pending or completed **proceedings**; and
- even **legacy audit objections** raised in the case.

Because it draws this material together automatically, the 360° View is central to the **collection and verification of data pertaining to the assessee**: an officer can cross-check what the taxpayer has declared against the Department's own records, spot inconsistencies across years, and confirm the completeness of the case record before issuing a notice or passing an order. The facility is not confined to Common Functions alone; the 360° View is surfaced within **several ITBA functionalities** (for example, from the Assessment, Rectification, Recovery and related modules), so that the officer can call up the consolidated profile at the point of work without leaving the task in hand.

Authenticating communications — DSC and DIN

Digital Signature Certificate (DSC) on ITBA

What it is. A **Digital Signature Certificate (DSC)** is the electronic equivalent of an officer's handwritten signature, backed by a cryptographic certificate issued to that officer and used through a signing token. Officers register for DSC (through HRMS) and are issued a signing token; ITBA then lets them **append their DSC** to notices and orders.

Why it matters. A DSC makes a system-generated order **legally authenticated** and tamper-evident, so the taxpayer can trust that the order genuinely came from the named authority and was not altered. For the Department it removes the need for wet-ink signing and enables fully paperless, faceless proceedings.

Document Identification Number (DIN) — what it is

A **Document Identification Number (DIN)** is a unique, computer-generated number that ITBA stamps on the body of every notice, order, letter, summons or other communication issued to a taxpayer (or any other person). It was made mandatory by **CBDT Circular No. 19/2019 dated 14 August 2019**, with effect from **1 October 2019**.

The DIN rule and its consequence

On or after 1 October 2019, **no** communication relating to assessment, appeals, orders, exemptions, enquiry, investigation, verification of information, penalty, prosecution, rectification, approval, etc. may be issued **without a computer-generated DIN** quoted in its body. A communication issued without a DIN is treated as **invalid and deemed never to have been issued**. In exceptional situations a communication may go out manually, but only after recording reasons in writing and obtaining prior written approval of the CCIT/DGIT concerned; even then a DIN/Document Number is subsequently generated and an intimation carrying it is issued (this facility for manually-uploaded documents was enabled in ITBA from 25 October 2019).

Why DIN matters — to the taxpayer and the Department

- **To the taxpayer:** the DIN lets the recipient **verify authenticity** — a genuine departmental communication is traceable in the system, so fake or unauthorised notices can be exposed and rejected. It is a transparency and anti-fraud safeguard.
- **To the Department:** DIN creates a complete, auditable record of every communication (who issued what, when, to whom), enforcing accountability and standing up to judicial scrutiny — several tribunals have quashed DIN-less orders, underlining how significant this control is.

The wider ITD application ecosystem

ITBA does not stand alone. It is one member of a family of systems, each serving a distinct audience.

System	Audience / role	One-line purpose
ITBA (itba.incometax.gov.in)	Departmental officers/staff	Officer-facing platform for assessment, PAN/TAN, TDS, penalty, recovery, appeals, etc.
e-Filing portal (incometax.gov.in)	Taxpayers & professionals	File ITRs and forms, respond to notices (e-Proceedings), e-verify, view AIS, lodge grievances, apply for e-PAN.
CPC-ITR, Bengaluru	Back-office (centralised)	Bulk processing of ITRs u/s 143(1), refunds and intimations.
CPC-TDS / TRACES (tdscpc.gov.in)	Deductors, taxpayers, AO(TDS)	TDS statement processing, Form 16/16A, Form 26AS, defaults and justification reports.
Insight (Project Insight)	Officers (risk/verification)	Data analytics, risk scoring, AIS, information for verification and case selection.
e-Proceedings / e-Nivaran	Taxpayers ↔ officers	Paperless conduct of proceedings; grievance receipt and redressal.
Protean (ex-NSDL e-Gov) & UTIITSL	Intermediaries	ITD-appointed agencies for physical PAN/TAN application receipt and processing.

The e-Filing portal — what it is and why it matters

What it is: www.incometax.gov.in is the Department's public, taxpayer-facing portal where individuals, businesses and professionals register, file returns and statutory forms, **respond to notices through e-Proceedings**, **e-verify** returns, view their **AIS**, apply for **e-PAN**, and raise grievances. **Why it matters:** it is the single window between the taxpayer and the Department. Its integration with ITBA is what makes **faceless, paperless** interaction possible — the officer's notice raised in ITBA surfaces to the taxpayer here, and the taxpayer's reply flows back to the officer's ITBA worklist. For the Department it is the authoritative intake point for returns and responses.

CPC-ITR (Bengaluru) — what it is and why it matters

What it is: the **Centralised Processing Centre for Income-Tax Returns** at Bengaluru performs high-volume, automated processing of filed ITRs **under section 143(1)**, generating intimations and refunds without an officer handling each return. **Why it matters:** it delivers fast, consistent, arithmetic-and-cross-check processing at national scale, freeing field officers to focus on scrutiny/verification. Cases needing officer action (e.g., scrutiny, or certain post-processing functions) are then handled in ITBA. For the taxpayer it means quicker refunds and standardised intimations.

CPC-TDS / TRACES — what it is and why it matters

What it is: TRACES (TDS Reconciliation Analysis and Correction Enabling System, tdscpc.gov.in) is the TDS ecosystem run by CPC-TDS. Deductors file and correct TDS statements here; it generates **Form 16/16A**, powers **Form 26AS**, and flags **defaults** and justification reports; AO(TDS) uses it alongside the ITBA TDS module. **Why it matters:** it reconciles tax deducted by payers with credit claimed by taxpayers. For the taxpayer, correct TDS reflected in Form 26AS/AIS is essential to getting credit and refunds; for the Department it is the backbone of matching and TDS enforcement.

Insight (Project Insight) — what it is and why it matters

What it is: Insight is ITD's data-analytics and risk-management platform. It ingests information from many sources (e-Filing, TDS statements, **SFT/reporting entities**, data-exchange partners, ITD users), normalises it, **risk-scores** anomalies, matches it against ITRs and the **AIS**, and drives **e-verification**, case selection and campaigns. (The original Project Insight operations phase concluded on 31 March 2025, and Insight 2.0 commenced on 1 April 2025.) **Why it matters:** it targets the Department's limited enforcement effort at genuine risk, reducing intrusive scrutiny of compliant taxpayers. For the taxpayer it underlies the AIS/e-verification "nudge" approach — a chance to correct or explain before formal action; for the Department it is the engine of data-driven, non-adversarial compliance.

How the systems fit together — the data flow

A typical journey shows the systems working as one chain:

1. the taxpayer **files** the return on e-Filing;
2. **CPC-ITR** processes the return under s. 143(1) and issues an intimation or refund;
3. **TRACES** supplies the TDS credits reflected in Form 26AS/AIS;
4. **Insight** risk-scores the case and may flag it;
5. selected/scrutiny and post-processing cases land in the officer's **ITBA** worklist;
6. the officer's DIN-bearing, DSC-signed notice issues through **e-Proceedings** back on e-Filing; and
7. the taxpayer's response returns to the officer's ITBA worklist.

Data flows between the systems automatically instead of being re-keyed.

The major ITBA modules at a glance

Module	Purpose
PAN	Allotment, correction, transfer, de-duplication and management of PANs (s. 139A).
TAN	Allotment and management of Tax Deduction & Collection Account Numbers (s. 203A).
TDS	AO(TDS) functions — surveys, default follow-up, processing and recovery, linked to TRACES.
ITR Processing	AO-level handling of returns and CPC-pushed cases around s. 143(1).
Assessment	Scrutiny/faceless assessment; notices u/s 143(2)/142(1); orders u/s 143(3)/144/147; s. 131/133/142(2A) powers.
Rectification	Correction of mistakes apparent from record (s. 154).
Recovery	TRO functions — demand collection and recovery (s. 220–226), attachment, certificates.
Audit	Internal/Revenue/Statutory audit objections, settlement and remedial action.
Penalty	Initiation and levy of penalties (e.g., s. 270A, 271-series, 272A).
Appeal	CIT(A)/JCIT(A) appellate proceedings and effect of appellate orders.
OGE (Order Giving Effect)	Passing orders to give effect to appellate/revisionary/court directions.
DRP / MAP	Dispute Resolution Panel objections; Mutual Agreement Procedure proceedings.
e-Nivaran	Receipt, allocation and disposal of taxpayer grievances.
Common Functions	Shared services — jurisdiction, worklist, notings, DSC, DIN, letters, document management, 360° View.
MIS	Reports, dashboards and monitoring of pendency/disposal.

Legal & procedural references

- **Income-tax Act, 1961:** s. 139A (PAN); s. 203A (TAN); s. 143(1) (processing); s. 143(2)/142(1) (scrutiny notices); s. 143(3)/144/147 (assessment); s. 154 (rectification); s. 156 (notice of demand); s. 220–226 (collection & recovery); s. 250 (appeal); s. 270A/271-series/272A (penalty); s. 131/133/142(2A) (assessment powers).
- **DIN: CBDT Circular No. 19/2019 dated 14.08.2019**, effective 01.10.2019 — mandatory computer-generated Document Identification Number on departmental communications; DIN-less communications invalid/deemed never issued; manual issue only with recorded reasons and prior written approval of the CCIT/DGIT.
- **ITBA Instructions** issued by the **Directorate of Income Tax (Systems) / Pr. DGIT(Systems)** governing rollout, login (RSA token over TAXNET), and module functioning (e.g., Common Functions and Assessment module instructions).
- **PAN/TAN agencies:** ITD-appointed **Protean eGov Technologies Ltd (formerly NSDL e-Governance)** and **UTIITSL**.
- **Project Insight / Insight 2.0** for risk analytics, AIS and SFT-based information.
- **Legacy ITD/AST (and TMS)** — the pre-ITBA client-server platform that continues to hold records and computations for very old cases; relevant where old years are revived after litigation (e.g., the

Hexaware Technologies line on s. 148 notices and s. 151A JAO/FAO jurisdiction — in further appeal as of FY 2025-26).

Key Takeaways

- **ITBA** (https://itba.incometax.gov.in) is the ITD's single, integrated, **officer-facing** platform; the **e-Filing portal** (incometax.gov.in) is the **taxpayer-facing** one. Keep the two worlds distinct.
- ITBA **replaced the legacy AST/ITD application**, curing isolated databases, missing workflow, weak integration and thin audit trails.
- Access is only over **TAXNET** (or **SSL-VPN**); login is **two-factor** — departmental user-id + password **plus** a personal **RSA SecurID token**.
- **SSO** = authenticate once, reach all authorised modules. Never share the RSA token or credentials — it is a core security control protecting taxpayer data.
- Work reaches an officer as **work-items** in a **Worklist**, routed by **jurisdiction** and **hierarchy**; items move with the PAN on transfer, and every action is recorded in **Case History/Notings**.
- **Common Functions** supplies the shared services (jurisdiction, worklist, DSC, DIN, document management, **360° View**) used by every module; **MIS** provides reports and dashboards.
- The **360° View** consolidates an assessee's full profile — prior assessments and reassessments, appeals, refunds, income profiles, demands/proceedings and even legacy audit objections — on one screen; it is the principal tool for **comparative analysis** and for collecting/verifying data on the assessee, and is available within several ITBA functionalities.
- The **legacy ITD/AST application** (with **TMS** at unconnected stations) preceded ITBA and still holds data, records and computations for very old cases; such cases occasionally need action today (e.g., old years revived after litigation such as the *Hexaware* line), so officers should understand its basic operation and where legacy data resides. A DIN for a legacy ITD/AST order is generated within that application, not from ITBA Common Functions.
- Every communication carries a **DIN** (CBDT Circular 19/2019, from 01.10.2019); a **DIN-less** communication is **invalid/deemed never issued** — a key authenticity safeguard for taxpayer and Department alike. Orders are authenticated with a **DSC**.
- **CPC-ITR, Bengaluru** does bulk processing u/s **143(1)**; **CPC-TDS/TRACES** (tdscpc.gov.in) handles TDS, Form 16/16A and Form 26AS; **Insight** provides risk analytics, AIS and SFT-based selection.
- The systems form a **chain**: e-Filing → CPC-ITR → TRACES → Insight → ITBA (officer) → e-Proceedings back to the taxpayer; data flows rather than being re-keyed.
- The two ITD-appointed **PAN/TAN intermediaries** are **Protean (ex-NSDL e-Gov)** and **UTIITSL**.

Key terms & abbreviations

- **ITBA** — Income Tax Business Application (officer-facing platform).
- **AST** — Assessment Information System (legacy, menu/parameter-driven assessment software); **ITD application** — the older client-server suite ITBA replaced; **TMS** — Tax Management System, the standalone software used at stations not yet on the network.
- **SSO** — Single Sign-On (authenticate once, all authorised modules).
- **RSA token** — RSA SecurID hardware/soft token generating a one-time code (the second authentication factor).
- **TAXNET** — ITD's private wide-area network; **SSL-VPN** — secure remote access into it.

- **DSC** — Digital Signature Certificate (electronic signature on notices/orders).
- **DIN** — Document Identification Number (unique computer-generated number on every communication; CBDT Circular 19/2019).
- **Work-item / Worklist** — a unit of pending work / the officer's electronic in-tray.
- **Common Functions** — shared-services module (jurisdiction, worklist, DSC, DIN, document management, 360° View).
- **CPC-ITR / CPC-TDS** — Centralised Processing Centre (Income-Tax Returns, Bengaluru / TDS).
- **TRACES** — TDS Reconciliation Analysis and Correction Enabling System (tdscpc.gov.in).
- **Insight** — ITD's data-analytics/risk-management platform (Project Insight → Insight 2.0).
- **AIS** — Annual Information Statement; **SFT** — Statement of Financial Transactions; **Form 26AS** — annual tax statement.
- **e-Filing portal** — taxpayer-facing portal (incometax.gov.in); **e-Proceedings** — paperless conduct of proceedings; **e-Nivaran** — grievance redressal.
- **AO** — Assessing Officer; **TRO** — Tax Recovery Officer; **OGE** — Order Giving Effect; **DRP** — Dispute Resolution Panel; **MAP** — Mutual Agreement Procedure.
- **Pr. DGIT(Systems)** — Principal Director General of Income Tax (Systems) / Directorate of Income Tax (Systems), which builds and runs ITBA.
- **Protean** — Protean eGov Technologies Ltd (formerly NSDL e-Governance); **UTIITSL** — UTI Infrastructure Technology And Services Ltd (PAN/TAN intermediaries).

02. ITBA Common Functions, MIS Reports, Email & Video Conferencing

Applicable to: ITO Paper-V, ITI Paper-IV, MS Paper-IV (all three cadres)

Syllabus reference: ITBA Applications Modules — (l) Common Functions; (m) MIS-REPORT generation across all modules; (n) Email & Video Conferencing (VC).

Overview

The **Income Tax Business Application (ITBA)** is the Department's integrated, web-based, workflow-driven platform on which every functional line of work runs — Assessment, Penalty, Appeal, Recovery, Audit, Exemption, TDS, Investigation and more. Sitting *underneath* all of these is the **Common Functions** module: not a proceeding module of its own, but a layer of **shared utilities** that every other module re-uses. If you understand Common Functions — how a task reaches an officer, how a notice is generated, signed and served, how the file's "note sheet" is kept, and how supervisors watch pendency — you understand the mechanics of operating *any* ITBA module. This chapter therefore also teaches the vocabulary (worklist, workitem, DMS, DSC, DIN, notings, MIS, VC) that recurs throughout the rest of the paper. Common Functions is reached from the **ITBA Portal → Login → Modules tab → Common Functions**.

What ITBA is and how it works

ITBA converts the entire paper-file life-cycle into an electronic workflow, and that workflow model — the **workitem** in a **worklist** — is the single design idea from which pendency, MIS and monitoring all follow.

From the paper file to electronic workflow

Before ITBA, a case moved as a **physical file** carried by hand between the Assessing Officer (AO), the Range and the CIT, with a paper note sheet, paper notices and a manual dispatch register. ITBA converts that entire life-cycle into an **electronic workflow**: a case is a record in a database, an action is a transaction, and movement between officers is the routing of an electronic **workitem**.

- **Why it matters to the Department:** every action is time-stamped, attributable to a user, and centrally visible — enabling supervision, MIS, and audit without registers. It also integrates with **e-Filing** so notices reach the taxpayer's account instantly.
- **Why it matters to the taxpayer:** faster, traceable service of notices; a single online window (e-Filing / e-Proceedings) to receive communications and file responses; and a documentary trail if a dispute arises over whether/when a notice was served.

Workitem and Worklist

ITBA is **workflow-based**. Every task an officer must act upon is pushed to them as a workitem sitting in their worklist.

- A **work item** is a single pending action — a notice to issue, a draft order to approve, a Seek-Information request to answer, a hearing to conduct.
- A **worklist** is the officer's electronic in-tray: the list of all work items awaiting their action.
- To act on a workitem, the officer:

1. navigates to the worklist;
2. clicks the **hyperlink in the Subject column** to open the workitem;
3. reads the proceeding details shown; and
4. takes an action using the buttons provided.

Why the workflow model matters

Because a task *is* a worklist item, pendency ceases to be an abstraction and becomes a concrete, measurable quantity attributable to a specific officer. When a workflow is initiated, **pendency is created in the worklist of the assigned/initiating officer**. This single design choice is what makes MIS, pendency monitoring and time-barring alerts possible, and it lets supervisors see the workload pending with each officer without having to ask.

Actions available on a workitem

Actions are partly **module-specific** and partly **generic (common across modules)**. The common ones include **Delegate**, **Submit** (to senior), **Send Back**, **Approve**, **Cancel**, **Transfer**, **Hearing**, and **Case History / Notings**.

- **Delegate** — assign a workitem to your **Headquarters/staff** (e.g. AO delegates data entry to an Inspector/TA). **Bulk Delegation** of many workitems at once is available directly from the worklist.
- **Submit to Senior / Send Back** — route a draft order up for approval, or return it for correction.
- **Pull Back / Send Reminder** — recall a delegated item, or nudge a pending one.
- The user can also **switch between worklists** of different modules from a single screen.

The Note Sheet: Case History / Notings

The **Case History / Notings** screen is ITBA's electronic note sheet — both the concept and the day-to-day screen.

What it is and why it matters

On a paper file, the **note sheet** (or "notings") is the running left-hand record where each officer writes what was done and what is proposed, in date order, before the file moves on. It is the memory and the reasoning trail of the file.

- **What it is in ITBA:** the **Case History / Notings** screen is the electronic note sheet of a proceeding — a chronological, system-maintained record of *every* action taken on the case.

- **Why it matters to the Department:** it is a **tamper-evident audit trail**. Because entries are generated by the system on each event (notice issued, response received, order passed, email delivery status, seek-information replies), the record cannot be quietly back-dated or edited, which protects the officer and supports supervisory and vigilance review.
- **Why it matters to the taxpayer:** the taxpayer's replies and attachments filed on e-Filing land here and are demonstrably on record, so a response cannot later be treated as "not received".

The screen in practice

- The AO / AO staff click **Case History Notings** to view the complete action trail of a case, with attachments.
- Every material event auto-creates a **notings entry** in the relevant proceeding.
- Any **response from the taxpayer** (with attachments) filed through e-Filing is visible in the Case History / Notings of the relevant ITBA proceeding.
- Notings are visible to the proceeding owner and, for monitoring, **up the hierarchy** (Range/CIT/PCIT).
- Note the division of labour: an initiator can *view* an exchange (e.g. Seek Information) from Notings, but *action* on it can only be taken from the originating workitem.

Document management: DMS and document generation

ITBA stores every document once in a central repository and generates statutory communications from standard templates.

Document Management System (DMS) — what it is and why it matters

- **What it is:** the **DMS** is ITBA's central document repository. Every scanned or uploaded document — a taxpayer reply, an internal record, a manually issued notice — is stored once and **attached to the relevant workitem/proceeding**.
- **Why it matters to the Department:** documents are **retrievable across modules** and are carried in the Notings, so the same PDF the AO signed is the PDF in the file, in DMS, and with the taxpayer — eliminating divergent paper copies and "missing document" disputes. It underpins the Department's "going paperless" objective.
- **Why it matters to the taxpayer:** the exact document served on them is preserved and reproducible, and their uploaded evidence is safely on record.

Generating notices, letters and orders from templates

Statutory communications are **generated from standard system templates**, so the format, legal references and mandatory particulars are correct and uniform.

- The **List of Notices, Orders and Letters** is available **under each module** and shows all **Letters, Notices, Questionnaires and Orders** issued by any officer, for PANs in the user's jurisdiction.
- From this screen the user can **View / Download** and **Re-generate** previously generated documents; a letter can be **copied to multiple entities** at once.
- Both **system-generated** and **manually added** notices/orders are tracked here. Documents generated by **CIT(A) / TPO are visible to AO, Range, CIT, CCIT and PCCIT** for monitoring.

Signing and identifying documents: DSC and DIN

Two distinct credentials govern every outward communication: the **DSC** *authenticates/signs* the document, and the **DIN** *identifies and registers* it in the system. Do not confuse them.

Digital Signature Certificate (DSC) — what it is and why it matters

- **What it is:** a **DSC** is a cryptographic credential, issued by a licensed Certifying Authority and held on a physical **USB token**, that binds a document to the signer's identity and guarantees the document was not altered after signing. Under the **Information Technology Act, 2000 (ss. 3 & 5)** a digitally signed document has the same legal validity as a hand-signed one.
- **Why it matters to the Department:** it lets orders and notices be issued **paperlessly and remotely** yet authentically — essential for faceless and e-proceedings — and it fixes accountability, since the signature identifies the exact officer.
- **Why it matters to the taxpayer:** they can rely on a digitally signed PDF as a genuine, unaltered communication from the named authority, and can verify it.

DSC registration and use in ITBA

- Officers **register their DSC through HRMS** against their designation; the **DSC token is issued to the officer** (registration is covered in the HRMS session, not Common Functions).
- The same DSC is used to **sign orders, notices and letters in ITBA** and to **digitally sign APAR and IPR in HRMS**.
- The signed document is **sent directly from the application by email as an attachment**, and the **same document is available in ITBA and with the taxpayer**, eliminating the need for a printout.

Signing at issue, or "sign later"

- At **Issue**, the officer may sign immediately (insert token → sign) or opt to **sign later**.
- **Golden rule:** *unless the document is digitally signed, it will NOT be emailed and will NOT be shared with e-Filing under e-Proceedings.*
- If signing is deferred, the item goes to the **Dispatch Register → Sign Later** and the email is held. To complete the signing later, the officer:

1. opens the **Dispatch Register**;
2. selects the document;
3. appends the DSC (inserting the token); and
4. clicks **Sign**.

- If the officer **cancels** the signature after the notice is generated, an entry is added to the Dispatch Register to **Sign Later**, the **email is stopped**, a confirmation message is shown, and the button is disabled.

Document Identification Number (DIN) — what it is and why it matters

- **What it is:** the **DIN** is a unique, computer-generated identification number that ITBA stamps on the **body of every outward communication** — notice, order, summons, letter, correspondence. (Do not confuse it with the **DSC**: the DSC *authenticates/signs* the document; the **DIN identifies and registers** it in the system.)
- **Why it exists: CBDT Circular No. 19/2019 (dated 14.08.2019)** made DIN mandatory for all such communications issued **on or after 01.10.2019**. Any communication issued **without a DIN** (outside the narrow exceptions) is **invalid and deemed never to have been issued**. The aim is transparency, an audit trail and the elimination of fake or off-system notices.
- **Why it matters to the taxpayer:** a genuine notice will carry a DIN the taxpayer can **verify on the e-Filing/incometax portal**; the absence of a DIN is a strong signal of a fraudulent or defective communication, and has been a successful ground of challenge before Tribunals and High Courts.

- **Why it matters to the Department:** every outward paper is centrally logged; manual issue is permitted only in listed exceptional circumstances, with **prior written approval and reasons**, and must be **regularised on the system within the prescribed time** (DIN generated and intimated to the recipient).

Currency note on DIN

Circular 19/2019 is the instruction that the ITBA workflow reflects and that governs the FY 2024-25 / AY 2025-26 period. It has since been **superseded by CBDT Circular No. 4/2026 (31.03.2026)**, which restates the DIN mandate (clarifying that the DIN need not appear on every page and may be carried in the covering email or an attached document) and aligns it with the new **s. 292BA** referencing framework. For the current exam, know the **principle and Circular 19/2019**; be aware the 2026 circular is the latest position.

Dispatch and service of notices (Dispatch Register)

The **Dispatch Register** controls the actual service of every outgoing document and is the officer's proof of service.

- **Digitally signed** documents are **sent by email** (from the officer's designation email) and **shared with e-Filing** for service under e-Proceedings on the taxpayer's e-Filing account.
- **Dispatch manually without DSC:** use **View/Edit Dispatch Register → Physically Dispatch**; the document is then shared with e-Filing and the email is sent (if "send email" was ticked at issue), recording manual/physical service.
- The register lets the officer **enter Dispatch Date and Service Date** (individually or **in bulk**), **track the status of the sent email**, **digitally sign documents**, and **manually dispatch documents pending DSC**.
- Because the register records dispatch date, status and delivery, it evidences **valid service of notice** under **s. 282 read with Rule 127** (modes of service), which is often decisive in appeals about limitation and validity.

Seek Information (online internal information request)

A shared **ad-hoc / suo-moto workflow** for **calling for information online from other users within the Department** (e.g. an AO seeking inputs from a subordinate or another charge; the same mechanism underpins RTI workitems).

- To raise a request, the initiator:

1. performs **Search and Select Officer**;
2. enters the **Subject, Reference, Information Sought, PAN/TAN (if applicable) and a Compliance Date**; and
3. clicks **Initiate**.

- The request appears as **pendency in the addressee's Common Functions worklist**; the addressee opens it, enters a response (with attachments) and submits.
- The response returns to the **initiator's Common Functions worklist**; the initiator can view **Response History**, then **Close** the workitem or **seek further information**.
- Throughout, the full exchange is recorded in the **Case History / Notings** of the relevant proceeding (viewable there, but actionable only from the workitem).

Search, calendar, reminders and pendency monitoring

Common Functions also provides the everyday locate-and-supervise utilities used before and after acting on a case.

Taxpayer search, calendar/diary and reminders

- **Search criteria** (PAN, AY, TAN, name) let an officer locate a taxpayer record/proceeding before acting; **"No details available"** appears if the record is outside their jurisdiction.
- **Calendar / diary** functions flag **compliance dates and hearing dates**; **reminders** can be sent for pending workitems.

Pendency monitoring by supervisors

Because every task is a worklist item, **senior officers can monitor PENDING and CLOSED workitems for their charge** — supervision without paper registers. Delegated and submitted items remain visible up the chain, so a Range Head/CIT can see stalled items and intervene.

MIS Reports (Management Information System) — what it is and why it matters

- **What it is: MIS Reports** and **Dashboards** are the analytical, read-only outputs generated by every ITBA module from the same transaction data that drives the workflow.
- **Why supervisors need them:** an officer cannot open thousands of individual worklists to run a charge. MIS aggregates the data so that supervisors can **Track Daily Progress, Monitor & Direct, and make Effective Decisions** — spotting **time-barring** cases, uneven workloads, stalled pendency and disposal shortfalls at a glance.
- **Why it matters to the taxpayer (indirectly):** better monitoring means fewer cases drifting to time-bar, faster grievance disposal, and more even, accountable administration.

Accessing and using MIS

- MIS Reports are accessed from each module's **Home Page** → **MIS Reports** section (e.g. the **e-Nivaran** MIS).
- Reports allow selection by **PAN, AY, period, officer** etc., and typically give **work done, pendency, ageing/time-barring analysis, and disposal statistics**.
- **Example:** the e-Nivaran **Pending and Disposed Grievances dashboard** shows **zone-wise counts and ageing analysis** of grievances pending with an officer.
- Primary users are **Range Head / CIT / PCIT** for pendency, ageing and disposal review.

Email and Video Conferencing

ITBA both delivers signed communications by email and hosts the personal hearings that keep faceless proceedings compliant with natural justice.

Email from ITBA

- ITBA sends notices/letters/orders as **signed PDF attachments directly from the application**, using the **officer's designation email ID** (not a personal ID), so continuity survives transfers.
- **Delivery status is logged back into the Case History / Notings** of the parent workitem, so the officer can track whether the email was sent/delivered.
- Recall the **golden rule**: email goes out **only after DSC signing** (or after physical dispatch is recorded).

Video Conferencing — what it is and why it matters

- **What it is:** a **VC / video-telephony facility** provided through ITBA/e-Filing for conducting **personal hearings** without the taxpayer physically visiting an office.
- **Why it matters:** it is the mechanism that reconciles **anonymity** (the essence of faceless proceedings) with **natural justice** (the right to be heard). The taxpayer speaks to and is heard by the unit conducting the assessment/appeal, without knowing or meeting the individual officer.

VC in faceless proceedings

- Under the **Faceless Assessment Scheme (s. 144B)** and the faceless appeal/penalty schemes, where the taxpayer requests an opportunity of personal hearing or to make oral submissions, **such hearing is conducted exclusively through video conferencing/video telephony** as per the CBDT/NaFAC procedure.
- The taxpayer **requests VC through their e-Filing account**; the officer joins from the ITBA/VC interface. Per NaFAC SOP the hearing is to be **granted promptly.**
- **Judicial position:** the personal-hearing right under **s. 144B(6)** has been treated as **effectively mandatory when requested** — the Bombay, Delhi and Madras High Courts have **set aside faceless orders** passed without granting a requested VC hearing, as a breach of natural justice.

Legal & procedural references

- **Income-tax Act, 1961:** s. **139A** (PAN); s. **144B** (Faceless Assessment; VC personal hearing, esp. **144B(6)**); ss. **143(2) / 142(1)** (notices); s. **156** (demand); s. **282** & **Rule 127** (modes/service of notice); s. **250** (faceless appeal hearing); s. **292BA** (DIN referencing framework — as amended, Finance Act 2026).
- **Information Technology Act, 2000** — ss. **3 & 5** (legal recognition of digital signatures / DSC).
- **CBDT Circular No. 19/2019 (14.08.2019)** — mandatory generation and quoting of **DIN** (superseded by **Circular No. 4/2026**, 31.03.2026).
- The ITBA Common Functions series of instructions issued by the **Directorate of Income Tax (Systems)**; CBDT/NaFAC **Faceless Assessment / Appeal / Penalty** Schemes, directions and SOP.

Key Takeaways

- ITBA is **workflow-driven**: a **workitem** = one pending task; a **worklist** = the officer's electronic in-tray. Initiating a workflow **creates pendency in the assigned officer's worklist** — the basis of all MIS and pendency monitoring.
- **Common Functions** is a shared-utility layer re-used by every module; reached via **Modules tab → Common Functions**. Learning it teaches how any ITBA module is operated.
- **Case History / Notings = the electronic Note Sheet** — a tamper-evident, chronological audit trail; taxpayer responses filed on e-Filing appear here.
- **DMS** stores every document once and attaches it to the proceeding, retrievable across modules and carried in Notings ("going paperless").
- **DSC ≠ DIN.** DSC (IT Act ss. 3/5, on a USB token, registered via **HRMS**) **signs/authenticates**; **DIN** (CBDT Circular 19/2019) **identifies/registers** the communication — a notice without DIN is **invalid**.
- **Golden rule of dispatch:** an **unsigned** document is **neither emailed nor shared with e-Filing**; only after **DSC signing** (or **Physically Dispatch** via the Dispatch Register) is it served. The **Dispatch Register** is the proof of service (s. 282 / Rule 127).
- **Seek Information** is an ad-hoc internal request with a **Compliance Date**, landing in the addressee's **Common Functions** worklist; the whole exchange is recorded in Notings.

- **Email** goes out as a **signed PDF from the officer's designation ID**, with delivery status logged to Notings.
- **MIS Reports & Dashboards** exist so supervisors can **Track Progress, Monitor & Direct, and Decide** — chiefly for pendency, ageing and **time-barring**.
- **Faceless personal hearings (s. 144B(6)) are held only by Video Conferencing**, requested via e-Filing, and are treated as **mandatory when requested** (High Courts quash orders that deny them).

Key terms & abbreviations

- **ITBA** — Income Tax Business Application (the Department's integrated case workflow platform).
- **Workitem / Worklist** — a single pending task / the officer's electronic in-tray of such tasks.
- **Notings / Note Sheet** — the Case History action trail of a proceeding.
- **DMS** — Document Management System (central document repository).
- **DSC** — Digital Signature Certificate (cryptographic signing credential on a USB token; registered via HRMS).
- **DIN** — Document Identification Number (unique computer-generated ID quoted on every outward communication).
- **MIS** — Management Information System (supervisory reports & dashboards).
- **VC** — Video Conferencing (video telephony used for personal hearings).
- **e-Filing / e-Proceedings** — taxpayer portal / electronic proceedings for service and response.
- **Dispatch Register** — the module controlling signing, dispatch and service of outgoing documents.
- **NaFAC** — National Faceless Assessment Centre.
- **HRMS** — Human Resource Management System (DSC/role registration; APAR/IPR signing).

Part II — Taxpayer Registers: PAN, TAN & TDS

03. PAN in ITBA

Applicable to: ITO Paper-V, ITI Paper-IV, MS Paper-IV (all three cadres).

Syllabus reference: ITBA Applications Modules — PAN and TAN: View / Update NRI Status details, Event Marking, Initiate Deletion / de-duplication / Restoration, Transfer / Create Transfer Order, Bulk Transfer. *(This chapter covers the PAN side only; TAN is dealt with in a separate chapter.)*

Overview

The **Permanent Account Number (PAN)** is the 10-character alphanumeric identifier issued by the Income-tax Department under **section 139A** of the Income-tax Act, 1961. It is the single most important key in the Department's data architecture: every return, challan, TDS entry, financial-transaction report (SFT), refund and assessment order is threaded to a PAN. In **ITBA (Income Tax Business Application)** and in the systems that feed it — Insight, TRACES, and CPC-ITR — the taxpayer's entire record is retrieved and reconciled through the PAN. This chapter explains, from first principles, **what PAN is and why it matters**, decodes the 10-character structure, walks through the allotment channels, and then breaks the **PAN Module of ITBA** into its many officer-facing functions: viewing and updating core data and NRI status, marking events, initiating deletion and restoration, resolving duplicate PANs (de-duplication), and transferring jurisdiction (single, by order, or in bulk). Legal consequences — inoperative PAN, penalties — are explained alongside.

What PAN is — and why it is the backbone identifier

What it is. PAN is a permanent, nationwide, 10-character alphanumeric number (format AAAAA9999A) allotted by the Income-tax Department to a person under section 139A. It is issued on a laminated/electronic card carrying the holder's name, father's name (for individuals), date of birth/incorporation and photograph. Once allotted, it stays with the person **for life** — it does not change with a change of address, name, jurisdiction, or assessing officer, and it is not reissued on death (it is instead closed via event marking/deletion).

Why it matters to the taxpayer. PAN is **mandatory** to file an income-tax return, to pay tax (challans), to claim TDS credit and refunds, and to enter into the high-value transactions listed in Rule 114B (opening bank accounts, buying property or vehicles, large cash deposits, securities dealings, etc.). Without a valid, operative PAN the taxpayer suffers **higher TDS/TCS** and cannot transact smoothly. It is, in effect, the citizen's tax identity.

Why it matters to the Department. PAN is the **primary key** that links every fragment of data about a taxpayer scattered across returns, TDS statements, SFT/AIS feeds, foreign-remittance reports and third-party data. This linkage is what enables **360-degree profiling** of a taxpayer, risk-based selection for scrutiny, non-filer monitoring (NMS), and the population of **Form 26AS/AIS/TIS**. If the identifier is wrong, duplicated or missing, the data cannot be joined and the Department's information advantage collapses. That is why the integrity of the PAN database — de-duplication, correct jurisdiction, accurate status — is a core administrative function, not a clerical one.

The 10-character structure decoded

PAN is in the form **AAAAA9999A** — five letters, four numerals, one letter. Each position carries meaning:

Position	Character	Meaning
1–3	Alphabetic	Running alphabetic series (AAA–ZZZ) allotted by the system
4	Alphabetic	**Status of holder** (category of person — see codes below)
5	Alphabetic	First letter of the **surname/last name** (individual) or of the **entity name** (non-individual)
6–9	Numeric	Sequential number (0001–9999)
10	Alphabetic	**Check digit** — an alphabetic checksum computed over the first nine characters

Fourth-character status codes: P – Individual; **C** – Company; **H** – HUF; **F** – Firm/LLP; **A** – Association of Persons (AOP); **T** – Trust; **B** – Body of Individuals (BOI); **L** – Local Authority; **J** – Artificial Juridical Person; **G** – Government.

Why the structure matters to an officer

The 4th and 5th characters allow an officer to verify a PAN at a glance: a PAN whose 4th character is **C** must belong to a **company**, and its 5th letter should match the first letter of the company name. A mismatch (e.g. an individual's return filed on a "C" PAN, or a surname initial that does not tally) is a red flag for a wrong or fabricated PAN. The **check digit** allows software to reject a mistyped PAN before it ever hits the database, preventing data being posted to a non-existent account.

Allotment of PAN

PAN may be allotted through several channels; ITBA receives and stores the resulting record and runs built-in duplicate validations before a fresh PAN is finalised.

Allotment channels

- **Protean eGov Technologies (formerly NSDL e-Gov)** — Form **49A** (Indian citizens and Indian entities) or Form **49AA** (foreign citizens/NRIs and entities incorporated abroad), under **Rule 114**.
- **UTI Infrastructure Technology And Services Ltd (UTIITSL)** — same forms 49A/49AA.
- **Instant e-PAN** via the **e-Filing portal (incometax.gov.in)** — free, paperless, Aadhaar-based (OTP) allotment for resident individuals who do not already hold a PAN; an electronically authenticated **e-PAN** (PDF with QR code) is issued in minutes.

What e-PAN is and why it matters

An e-PAN is a digitally signed Permanent Account Number (PAN) that is issued instantly and free of cost through the e-Filing portal using Aadhaar-based e-KYC. During the application process, the applicant's name, date of birth, gender, and address are automatically fetched from Aadhaar, and the applicant confirms the details through an OTP-based authentication process.

The introduction of e-PAN has significantly simplified the PAN issuance process by eliminating the need for paper-based applications, reducing dependence on intermediaries, and minimising processing delays. This frictionless mechanism encourages first-time applicants to obtain a PAN, thereby supporting the expansion of the tax base. Since the PAN is generated using Aadhaar-based e-KYC, it is generally already linked with Aadhaar at the time of allotment, ensuring that it is immediately operative for tax-related purposes.

The allotment process and built-in validations

Within the Income Tax Business Application (ITBA), the allotment of a fresh PAN is carried out through the PAN Allotment Process, which is accessed through the Allot PAN menu function. On successful completion of the process, the system generates the Information of Allotted PAN.

The PAN allotment workflow incorporates built-in validation mechanisms designed to identify probable duplicate applications before a PAN is finalised. Where the system determines that the application is unique, the operator selects the Queue for Allotment option, following which the PAN is generated.

If the validation process detects a probable duplicate, the application is automatically routed to the PAN Duplicate Resolver, a designated system role responsible for examining such cases. Upon verification, the resolver may select Abort and Mark Duplicate, preventing the allotment of another PAN. These cases are reflected under the List of Identified Duplicates, and applications confirmed as duplicates are subsequently recorded in the Information of Duplicate Marked Requests.

These built-in validation checks constitute the Department's first line of defence against the issuance of multiple PANs to the same individual and play a critical role in maintaining the integrity and uniqueness of the PAN database.

AO code and jurisdiction

Every PAN is tied to an **AO Code**, which is a four-part address inside the Department's jurisdiction map:

Component	What it fixes
Area Code	The region/CCIT charge
AO Type	Ward / Circle / range type (e.g. W, C, ITO/DC)
Range Code	The Range within the charge
AO Number	The specific assessing officer/ward

Together these fix the **assessing officer and jurisdiction** that "owns" the PAN. In ITBA the jurisdiction is examined through the **PAN Other Details** section under the **PAN Details** tab: **- View PAN Jurisdiction Details** — the current AO/jurisdiction of the PAN. **- View PAN Jurisdiction History** — a chronological record of every jurisdiction transfer the PAN has undergone. **- View PAN Lifecycle Summary** — the full chronological lifecycle (allotment, core-field updates, events, transfers, deletion/restoration) in one place.

Why the jurisdiction link matters

Jurisdiction determines **who** can issue notices, assess, and pass orders for a taxpayer. If the AO Code is wrong, notices go from the wrong officer and can be challenged for want of jurisdiction; work also lands in the wrong worklist. Keeping the PAN's AO Code correct — and transferring it cleanly when the taxpayer moves or the case is reassigned — is therefore essential to the validity of proceedings.

Aadhaar linkage, quoting and consequences of PAN defaults

Aadhaar–PAN linkage and the inoperative PAN (Rule 114AAA)

What it is. Under **section 139AA**, every person who was allotted a PAN as on **1 July 2017** and is eligible to obtain Aadhaar must **intimate (link) their Aadhaar number**. This requirement is, however, **subject to conditions of residency and eligibility**: by **CBDT Notification No. 37/2017 dated 11 May 2017** it does **not** apply to persons in the exempted categories — namely a **non-resident** as defined under the Income-tax Act, a person who is **not a citizen of India**, an individual who is **eighty years of age or more** at any time during the previous year (a super-senior citizen), and a person residing in Assam, Meghalaya and Jammu & Kashmir (as specified in the notification; Jammu & Kashmir is now a Union Territory). Such persons are not required to link Aadhaar and are not exposed to the consequences of an inoperative PAN. For every other eligible person, if Aadhaar is not linked the PAN is rendered **inoperative** in the manner prescribed by **Rule 114AAA**.

Why it matters. An **inoperative** PAN is treated, for the period it remains inoperative, **as if the PAN had not been furnished at all**. The consequences (effective from 1 July 2023) are severe: **- TDS/TCS is**

deducted/collected at the higher rates under sections 206AA / 206CC; - **refunds are not issued**, and **no interest** runs on any refund for the inoperative period; - **returns cannot be processed** and **pending proceedings** (e.g. on defective returns) cannot be completed; - the holder cannot validly quote the PAN where quoting is required.

The PAN can be made **operative again** by linking Aadhaar with the prescribed **fee of ₹1,000** under **section 234H**. This is why officers must distinguish a genuinely inoperative PAN (non-linkage) from a deleted or fake PAN — the remedies are entirely different.

Quoting of PAN and Form 60

- **Quoting PAN is mandatory** in returns, challans, and the specified transactions listed in **Rule 114B** (e.g. high-value bank accounts, immovable property, securities, motor vehicles and large cash dealings).
- Where a person **does not hold a PAN**, a declaration in **Form 60** is furnished (proviso to Rule 114B).
- **Reporting entities** verify and record PAN/Form 60 under **Rules 114C–114D**, feeding this data back to the Department — another reason PAN integrity underpins the whole information system.

Penalty for PAN defaults — section 272B

Section 272B empowers the Assessing Officer to levy a penalty of **₹10,000** for PAN-related defaults — failing to comply with section 139A (including failure to obtain/quote PAN), **quoting a false PAN or Aadhaar**, or failing to authenticate PAN where required. Penalty is imposed after giving the person an opportunity to be heard, and may be waived for a **reasonable cause** shown to be bona fide.

Viewing and updating the PAN record

View PAN Details — reading the core record

View PAN Details (users: **AO, Range, CIT, CCIT**) displays the PAN's core fields — name, father's name, date of birth/incorporation, address, category/status, and **residential (NRI) status** — together with jurisdiction and the lifecycle summary. This is the read-only window an officer uses to confirm identity before acting on any proceeding.

Update PAN Details — processing changes to core fields

When a change request comes in for **core fields**, the officer processes it through **Update PAN Details** (users: **AO, Range, CIT, CCIT**): - The screen shows a **side-by-side comparison of the original core-field values against the change-request values**, with the changed fields **highlighted**, reached by clicking the PAN on the **PAN(s) for Update** screen. - The officer may **Request for confirmation / supporting documents** before accepting the change. - **Update validations again run de-duplication.** A flagged request is routed to the **PAN Duplicate Resolver** (under **Information of Duplicate Marked Requests**); the officer clicks **Mark Duplicate after linking the update request to the correct PAN** where duplicity is found. - **Pending update requests** awaiting action are listed on the **PAN(s) for Update** screen.

NRI / residential status — view and update

What it is. The residential status attribute records whether the holder is a **resident** or **non-resident (NRI)**. It is one of the maintainable core attributes of the PAN and is updated through the same Update PAN Details flow.

Why it matters. Getting the NRI flag right has real downstream effects: - it drives the **Form 49A vs 49AA** classification (Indian vs foreign applicant); - non-residents are taxed only on India-source income and face **different TDS/withholding** treatment (often higher rates and TDS on payments to non-residents under section 195); - it interacts with the **inoperative-PAN** rules — the CBDT has carved out relief so that a genuine NRI who has correctly intimated non-resident status is not wrongly rendered inoperative merely for not linking Aadhaar (an NRI may not be eligible for Aadhaar). Marking the status accurately therefore protects the taxpayer from wrongful higher deduction and protects the Department from misclassification.

Event Marking for PAN

What it is. Event Marking records a **significant occurrence** against a PAN so that the system and downstream users know the taxpayer's status has changed. Typical events include **death** of an individual, **dissolution/liquidation** of a firm/company, **amalgamation/merger**, marking a PAN as a **Fake Assessee**, or **linking** a PAN with a source/linked PAN.

Why it matters. Event marking stops the system (and officers) from treating a dead person, a dissolved entity, or a bogus PAN as a live, assessable taxpayer — preventing wrong notices, and flagging fraud (Fake Assessee) for special handling. It is reached from the **Event Details** tab.

Steps to mark an event

To mark an event, the officer: 1. selects the **Event Date** and the **Event Name**; 2. enters the **Source or Linked PAN** where the event involves another PAN; and 3. confirms the entry, whereupon the system returns "**Event Marked Successfully**".

Event functions and who can perform them

- **Mark Event** — user: **AO**.
- **Event History** — users: **AO, Range, CIT, CCIT, PCCIT** (view the log of events on a PAN).
- **Delete Event** — user: **AO**, **except** a **Fake Assessee** event, which **only the Global Administrator** can delete. This safeguard prevents an AO from quietly unmarking a PAN that has been flagged as bogus.

De-duplication, deletion and restoration

De-duplication — why duplicate PANs are a problem

What it is. De-duplication is the process of identifying, and marking, more than one PAN that in fact belongs to the **same person**, and consolidating on a single correct PAN.

Why duplicate PANs are a problem. Holding more than one PAN is **prohibited under section 139A(7)** and attracts penalty. Operationally, duplicates **fragment the taxpayer's record** — income, TDS and transactions get split across two identifiers, defeating 360-degree profiling and enabling a taxpayer to hide income or claim credits twice. Cleaning duplicates is therefore essential to data integrity.

How de-duplication is done in ITBA

When allotment or update validations throw up a **List of Identified Duplicates**, the officer (under the **PAN Duplicate Resolver** role) **links the request to the correct PAN** and clicks **Mark Duplicate** to flag the spurious PAN. The retained PAN is kept live; the marked duplicate is then typically routed into the **deletion** workflow. De-duplication thus feeds directly into deletion.

Initiate PAN Deletion

- **What it is.** Deletion permanently closes a PAN that should not exist — a spurious, erroneous or confirmed-duplicate PAN (usually the output of de-duplication).
- **How it works.** The **AO Initiates the Request for PAN Deletion**; a **workitem** is generated and flows through the **AO worklist** for approval before the PAN is actually deleted. Users: **AO, Range**.

Initiate PAN Restoration

- **What it is.** Restoration reverses a deletion, bringing a previously deleted PAN back to life where the deletion was made in error.

- **How it works.** Same design as deletion — the request generates a **workitem for restoration** that flows through the worklist/approval flow. Users: **AO, Range**.

Transfer of PAN jurisdiction

Transfer changes the **jurisdiction (AO)** that holds a PAN. This happens when a taxpayer moves, or when a case is administratively reassigned. ITBA supports both single-PAN transfer (with a formal order) and bulk transfer, and it distinguishes the two legal bases on screen: **Transfer u/s 120** and **Transfer u/s 127**.

Legal basis — section 120 vs section 127

- **Section 120** — jurisdiction of income-tax authorities; used where the change is one of **administrative/territorial vesting** of jurisdiction (a routine re-allocation flowing from CBDT/CCIT directions).
- **Section 127** — **power of higher authorities to transfer a case** from one AO to another. It requires a **recorded reason** and, where the AOs are not in the same city/locality, a **reasonable opportunity of being heard** to the assessee before the transfer.

Initiate Request for Transfer and NOC

- **Initiate Request for Transfer** (users: **AO, Range, CIT, CCIT, PCCIT**) — the **destination side** raises the request.
- **Obtain No Objection Certificate (NOC)** — an **NOC is obtained from the source AO** before the transfer proceeds, so the losing officer confirms there is no pending reason to retain the case.

Create Transfer Order

The competent authority generates the transfer order (users: **Range, CIT, CCIT, PCCIT**). Orders exist in two states: - **Draft** — identified by a **Draft Order No.**; - **Executed** — once approved, identified by a **Transfer Order No.**

View Transfer Order Details and Search Transfer Request

- **View Transfer Order Details** (users: **Range, CIT, CCIT, PCCIT**) — inspect **Draft** (via Draft Order No.) and **Executed** (via Transfer Order No.) orders.
- **Search Transfer Request** — locate pending transfer requests.

Bulk Transfer

Bulk Transfer moves **many PANs at once** (users: **AO, Range, CIT, CCIT, PCCIT, Nodal Officer, CIT(CO)**). PANs may be selected by any of four modes: - **From AO to AO** — move an entire AO's PANs to another AO; - **Based on Selection Criteria** — filter by attributes; - **Based on Address** — move PANs falling in a given address/area; - **Manually** — pick individual PANs.

View Erroneous PAN. Within Bulk Transfer, **View Erroneous PAN** lists the PANs that **cannot be moved** — those marked **Fake Assessee**, or those already locked in a **pending deletion, restoration or transfer** workflow. This prevents the bulk job from disturbing PANs that need special or sequential handling.

PAN Records Transfer (physical records)

Distinct from the electronic jurisdiction transfer, the movement of **physical case records** is tracked through the **PAN Worklist** (Subject = **"PAN Records Transfer"**), users: **AO (destination and source based)**: - the **Source AO** marks **Physical Records Sent**; - the **Destination AO** marks **Physical Records Received**.

This ensures that both the electronic jurisdiction and the physical file reach the same officer.

Legal & procedural references

- **Income-tax Act, 1961:** s.**139A** (allotment/requirement of PAN; **139A(7)** bar on holding more than one PAN), s.**139AA** (Aadhaar–PAN linkage), s.**120** (jurisdiction of authorities), s.**127** (transfer of cases), s.**195/206AA/206CC** (higher TDS/TCS where PAN absent/inoperative), s.**234H** (₹1,000 fee for late Aadhaar linkage), s.**272B** (penalty ₹10,000).
- **Income-tax Rules, 1962:** Rule **114** (application — Forms 49A/49AA), Rule **114AAA** (manner and consequences of inoperative PAN), Rules **114B–114D** (transactions requiring PAN, Form 60, and verification/reporting).
- **ITBA PAN Module functions:** Allot PAN (with duplicate validations → PAN Duplicate Resolver); View/Update PAN Details; NRI/residential status update; View Jurisdiction Details / History; View PAN Lifecycle Summary; PAN(s) for Update; Event Marking (Mark / Delete / Event History); Initiate Deletion / Restoration; De-duplication (Mark Duplicate); Initiate Request for Transfer / Obtain NOC / Create Transfer Order / View Transfer Order Details / Search Transfer Request / Bulk Transfer (4 modes + View Erroneous PAN); PAN Records Transfer (physical, via PAN Worklist).
- **Sources:** ITBA PAN Module documentation; incometax.gov.in (Link Aadhaar FAQ / Rule 114AAA); incometaxindia.gov.in (s.272B); CBDT Notification No. 37/2017 (s.139AA exemptions).

Key Takeaways

- **PAN is the backbone identifier** — the primary key linking every return, challan, TDS entry and SFT/AIS feed; its integrity is what enables the Department's 360-degree profiling, so de-duplication and correct jurisdiction are core (not clerical) functions.
- Format **AAAAA9999A**: **4th char = status of holder** (P=Individual, C=Company, H=HUF, F=Firm/LLP, T=Trust, A=AOP, etc.); **5th char = first letter of surname/entity name**; **10th char = check digit**. A mismatch is a red flag for a wrong/fake PAN.
- **Allotment channels:** Protean/UTIITSL via **Form 49A (Indian) / 49AA (foreign-NRI)** under Rule 114, and free Aadhaar-OTP **Instant e-PAN** via the e-Filing portal; ITBA's **Allot PAN** runs duplicate validations up front (Queue for Allotment vs Abort & Mark Duplicate).
- **Update PAN Details** shows original vs change-request core fields highlighted; **NRI/residential status** matters because it drives 49A/49AA, TDS/withholding on non-residents, and the inoperative-PAN carve-out for genuine NRIs.
- **Event Marking** flags death, dissolution, amalgamation, linked PAN and **Fake Assessee**; **Delete Event** is by AO **except Fake Assessee, which only the Global Administrator can delete**.
- **De-duplication:** more than one PAN is barred under **s.139A(7)**; the resolver **links to the correct PAN and clicks Mark Duplicate**, feeding the spurious PAN into the **deletion** workflow (deletion/restoration run through AO worklist workitems).
- **Transfer** changes the AO/jurisdiction under **s.120 (jurisdiction)** or **s.127 (transfer of case, with recorded reasons + opportunity of hearing)**; the **destination initiates** and an **NOC is obtained from the source AO**; orders go Draft (Draft Order No.) → Executed (Transfer Order No.).
- **Bulk Transfer** modes = **From AO to AO / Selection Criteria / Address / Manually**; **View Erroneous PAN** = Fake Assessee or PANs already in a pending deletion/restoration/transfer flow. Physical records: **Source marks "Sent", Destination marks "Received"**.
- **Inoperative PAN (Rule 114AAA / s.139AA):** unlinked Aadhaar makes the PAN inoperative — higher TDS/TCS, no refunds/interest, returns unprocessed; reactivate with **₹1,000 fee (s.234H)**.
- **Penalty s.272B = ₹10,000** for PAN default or quoting a false PAN/Aadhaar.

Key terms & abbreviations

- **PAN** — Permanent Account Number (10-char identifier under s.139A).
- **ITBA** — Income Tax Business Application.
- **AO Code** — Area Code + AO Type + Range Code + AO Number (fixes jurisdiction/assessing officer).
- **e-PAN** — instant, free, Aadhaar-OTP PAN issued via the e-Filing portal.
- **Form 49A / 49AA / 60** — PAN application (Indian / foreign-NRI) / declaration where no PAN is held.
- **Protean / UTIITSL** — authorised PAN service providers.
- **De-duplication** — identifying and marking spurious/duplicate PANs (**Mark Duplicate**).
- **PAN Duplicate Resolver** — system role that resolves probable duplicates flagged by validations.
- **Event Marking** — recording a significant event (death, dissolution, amalgamation, Fake Assessee, linked PAN) against a PAN.
- **Fake Assessee** — PAN flagged as bogus; special handling for deletion/transfer (only Global Administrator can delete the event).
- **Inoperative PAN** — PAN deactivated for non-linkage of Aadhaar (Rule 114AAA).
- **NOC** — No Objection Certificate obtained from the source AO before a transfer.
- **NRI / residential status** — resident vs non-resident attribute of the PAN, affecting form type and TDS treatment.
- **PAN Lifecycle Summary** — chronological record of a PAN's allotment, updates, events, transfers and deletion/restoration.

04. TAN in ITBA

Applicable to: ITO Paper-V, ITI Paper-IV, MS Paper-IV (all three cadres).

Syllabus reference: ITBA Applications Modules — PAN and TAN functions (TAN component).

Overview

Every person who deducts Tax at Source (TDS) or collects Tax at Source (TCS) needs an "account number" that identifies them to the Income Tax Department for the entire TDS/TCS machinery. That identifier is the **TAN — Tax Deduction and Collection Account Number** — a unique 10-character alpha-numeric code obtained under **section 203A** of the Income-tax Act, 1961. This chapter explains what TAN is and why it matters, how its 10 characters are decoded, who must obtain it (and who is exempt), how it is applied for (Form 49B / Rule 114A) through Protean (NSDL) or the e-filing portal, and how the jurisdictional officer manages the TAN through the **ITBA TAN Module** (allotment, update, closure, restoration, de-duplication, transfer, intimation letters and life-cycle tracking). It also covers the penal consequences of not obtaining or wrongly quoting TAN under **section 272BB**.

What TAN is and why it matters

What it is. TAN is a **10-character alpha-numeric number** allotted by the Income Tax Department to any person responsible for deducting or collecting tax at source. It is the deductor's/collector's permanent identity in the TDS/TCS ecosystem — quoted on every TDS/TCS challan, every quarterly statement (return), and every TDS/TCS certificate (Form 16/16A/27D).

Why it matters to the deductor/collector. TAN is legally mandatory (s. 203A). Without it a deductor cannot deposit TDS, cannot file TDS statements, cannot generate valid certificates, and exposes itself to penalty under s.

272BB. It is the deductor's single point of compliance for the whole year.

Why it matters to the deductee (the real taxpayer). TDS is money already paid to the government on the deductee's behalf. The **credit** for that TDS flows to the deductee's **Form 26AS / AIS** only when the deductor files a correct statement quoting the **correct TAN**. A wrong, duplicate or missing TAN breaks this chain — the deductee's tax credit does not appear, and refunds/assessments get stuck. TAN is therefore the pivot on which the deductee's TDS credit turns.

Why it matters to the Department. TAN lets the Department **track every deductor** as a distinct entity: monitor whether TDS is deducted and deposited on time, process quarterly statements, detect defaults, raise demands u/s 201/201(1A), and reconcile the tax the deductor withheld against what it deposited. It is the primary key that links deductor records across ITBA, the **TDS module**, **CPC-TDS** and **TRACES**.

TAN structure decoded, and TAN vs PAN

The 10-character TAN structure. A TAN follows the pattern **AAAA 99999 A** — four letters, five numerals, one letter.

Position	Characters	Meaning
1–3	Three letters	**City / jurisdiction code** of the location where TAN was applied — e.g. **DEL** = Delhi, **MUM** = Mumbai, **CAL** = Kolkata, **BLR** = Bengaluru
4	One letter	**Initial of the name** of the deductor/collector (individual or organisation)
5–9	Five numerals	System-generated **running serial number** (gives uniqueness)
10	One letter	System-generated **check / alphabetic** character (guards against typing errors)

Worked example: MUMA12345P — MUM = Mumbai jurisdiction; A = the deductor's name begins with A; 12345 = unique serial; P = check letter. Because the first four characters and the last character are alphabetic while the middle five are numeric, a TAN is readily distinguished from a PAN.

TAN and PAN compared. Both are 10-character numbers issued by the Income Tax Department, but they serve opposite ends of the same transaction and have different structures.

Aspect	TAN	PAN
Full form	Tax **Deduction/Collection** Account Number	**Permanent** Account Number
Purpose	Identifies the **deductor/collector** for TDS/TCS	Identifies the **taxpayer** for all income-tax purposes
Legal basis	Section **203A**	Section **139A**
Structure	**4 letters + 5 digits + 1 letter** → AAAA99999A	**5 letters + 4 digits + 1 letter** → AAAAA9999A
Application form	**Form 49B** (Rule 114A)	Form 49A / 49AA (Rule 114)
Used on	TDS challans, statements, certificates	Returns, transactions, KYC, etc.

A deductor typically holds **one PAN** (its own taxpayer identity) and **one TAN** (its deductor identity). The two are **linked** in ITBA — a single PAN can have one or more TANs mapped to it ("Linked TANs"), e.g. a company with separate TDS branches.

Who must obtain TAN, and where it must be quoted

- **Every person responsible for deducting TDS** (e.g. under ss. 192–195) or **collecting TCS** (s. 206C) must apply for, obtain and quote TAN — s. 203A(1).

- This covers **companies, firms, government offices / DDOs, local authorities, and individuals/HUFs** who are liable to deduct or collect tax.
- A deductor needs **only one TAN**. Holding or using more than one TAN for the same deductor is prohibited; extras are **duplicates** that the Department de-duplicates.

Where TAN must be quoted (section 203A(2)). Section 203A(2) requires the deductor/collector to quote TAN in: 1. all **TDS/TCS challans** for payment of tax; 2. all **TDS/TCS statements (returns)** filed; 3. all **TDS/TCS certificates** issued (Form 16, 16A, 27D); 4. all other **prescribed documents** / correspondence with the Department.

Persons NOT required to obtain TAN

Certain individual/HUF deductors are exempted so as not to burden small one-off transactions. They quote their **PAN** instead of a TAN and use a combined **challan-cum-statement**: - **Section 194-IA** — TDS on purchase of immovable property → **Form 26QB**. - **Section 194-IB** — TDS on rent by certain individuals/HUF → **Form 26QC**. - **Section 194M** — TDS on certain payments (contract/commission/professional fees) by individuals/HUF → **Form 26QD**.

Application for TAN — Form 49B under Rule 114A

- Application for allotment of TAN is made in **Form 49B** under **Rule 114A** of the Income-tax Rules, 1962.
- **Modes: online** through the Protean (formerly NSDL e-Gov) TIN portal, or through the **income-tax e-filing portal**; or **offline** at a **TIN-Facilitation Centre (TIN-FC)**.
- **Changes/correction** to existing TAN data are made through the separate **"Form for Change or Correction in TAN data"** (a TAN change request).
- On processing, the deductor receives a **TAN Allotment Letter / Intimation**. The allotment data then flows into the Department's systems, where the jurisdictional **AO (TDS)** views and maintains it through ITBA.

The ITBA TAN Module

The **TAN Module** in ITBA manages the end-to-end life-cycle of a TAN after allotment. From the **TAN Home Page**, users access the various processes: allotment validation, maintenance/view, update and closure, restoration, duplicity resolution, transfer, jurisdiction view, intimation letters and life-cycle summary. Access is role-based — the jurisdictional **AO (TDS)** and supervisory authorities operate the relevant screens, with actions routed as **workitems** through the ITBA worklist. The individual officer functions are set out below.

TAN Allotment (validation and queue for allotment)

When a fresh application is pending, the officer works the **TAN Allotment / Validation** screen: - The system runs **validations** on the application and produces a **List of Identified Duplicates** (possible existing TANs for the same deductor). - The officer opens the **Comparison** between the applied request and any linked/retained TAN. - **If the request is unique**, the officer clicks Queue For Allotment, and the application is queued for allotment. When the next **TAN Allotment batch** runs, the system generates and allots the TAN. - **If the request is a duplicate**, the officer selects it and clicks Mark Duplicate, and the application is rejected.

TAN Maintenance and View (read-only details)

The **TAN Maintenance** screen lets the officer search a TAN and click **View** to open the **TAN Details** screen. Tabs (read-only) include: - **Basic Details** (default) — core deductor data. - **Other Details** — including the **PAN** hyperlink that opens the **Linked TANs** view (all TANs mapped to that PAN). - **Nature of Payment/Collection (NOPC) Details** — the sections/natures under which the deductor deducts/collects. - **TDS Jurisdiction** — the mapped AO(TDS)/Range/CIT(TDS).

TAN Update and Closure

- On the **TAN Update and Closure Requests** screen, the officer clicks **Resolve** to open the **TAN Update and Closure** screen.
- For each update request the officer selects **Accept** or **Reject**; and to close TANs, ticks **Select for Closure**.
- Clicking Submit files the request.
- **Closure and pre-intimation.** On the **TAN Closure** screen, confirming with **Yes** changes the TAN status to Closed and enables **Generate Intimation Letter**. Where the **Request Type = Suo Moto** (closure initiated by the Department itself), a **Generate Pre Intimation Letter** facility is available to intimate the deductor before closure.
- **Aborting a closure.** The **TAN Pending For Closure** screen lists closures already initiated. Clicking the TAN hyperlink lets the officer either **Abort Closure** (cancel the initiated closure) or **Submit** to complete it. On abort, the closure against the TAN is cancelled.

TAN Restoration

If a TAN was closed wrongly or needs reactivation, the **TAN Restoration** screen restores it: on confirmation the status changes back to Active.

De-duplication of TANs

Why de-duplication matters. A deductor must hold **only one TAN**. Duplicate TANs cause TDS statements and challans to be split across two identifiers, so a deductee's credit can land under the "wrong" TAN and go missing from Form 26AS/AIS. Consolidating to a single retained TAN keeps the credit chain intact and the Department's deductor records accurate.

Procedure in ITBA. - On the **TAN Duplicity Resolution** screen, clicking the **Name** hyperlink opens the **TAN Duplicate Details** screen. - Clicking the **TAN** hyperlink there opens the **Comparison** between the **Duplicate TAN identified** and the **Linked (Retained) TAN**. - **If, after comparison, the request is unique**, the officer clicks **Queue For Allotment**. - **If it is confirmed a duplicate**, the officer selects the duplicate via checkbox and clicks **Mark Duplicate** → the duplicate application/TAN is **rejected**. - The **Retained TAN** is the one the deductor must quote thereafter; a **View Details of Retained TAN** link lets the officer inspect it. Duplicate TANs already in use should be **surrendered** by the deductor.

TAN Transfer (change of jurisdiction)

When a deductor's address/jurisdiction changes, the TAN must move to the correct **AO (TDS)**: - On the **TAN Transfer** screen the **Source AO** selects the TAN(s) via checkbox, chooses the **Destination AO** (search icon), enters remarks, and clicks **Transfer TAN(s)**. - A **TAN Transfer workitem** is created in the **TAN worklist** for necessary action. - The receiving officer clicks **Approve** or **Reject**. On approval, the TANs stand transferred to the jurisdiction of the Destination AO. - **Case History / Notings** records the full workflow trail. - **Transfer across RCC.** Transfer of a TAN across a **Regional Computer Centre (RCC)** boundary is supported through a dedicated screen (enter TAN → Transfer TAN(s)). A tracking screen shows the current status of cross-RCC transfer workitems and lets a user **re-assign** the approval task from one AO (AO1) to another (AO2) as applicable. The **Pending with** column shows who currently holds the workitem.

TAN Jurisdiction Details

The **TAN Jurisdiction Details** screen shows, by default, the **TDS Jurisdiction** tab (AO TDS / Range / CIT(TDS)). Additional tabs include **Jurisdiction Hierarchy**, **International Jurisdiction Hierarchy** (for TANs with international deduction jurisdiction) and a **History** tab showing the jurisdiction history for the TAN.

Generate TAN Allotment / Closure Intimation Letter

- On this screen the officer selects TANs from the list and clicks **Preview Intimation Letter** to view the draft letter for the first selected TAN.
- Clicking **Generate Intimation Letter** produces the allotment (or closure) letters for **all** selected TANs.

TAN Life Cycle Summary

The **TAN Life Cycle Summary** screen gives the complete history of a TAN — allotment, updates, transfers, closure and restoration — in one consolidated view, useful for audit and for resolving deductor grievances.

Linkage to the TDS module, CPC-TDS and TRACES

- The TAN is the **key** that ties the deductor to the **TDS module** in ITBA (processing of TDS/TCS statements, default identification, orders u/s 201) and to **CPC-TDS / TRACES** (TDS Reconciliation Analysis and Correction Enabling System) — the portal where deductors file/correct statements and download Form 16/16A and consolidated files.
- Correct, de-duplicated and correctly jurisdiction-mapped TAN data in ITBA is therefore **essential** for accurate TDS processing and for TDS credit to reach the deductee's **Form 26AS / AIS**.

Consequences of not quoting / not obtaining TAN (section 272BB)

- **Failure to apply for / obtain TAN** as required by s. 203A attracts a **penalty of ₹10,000 under section 272BB(1)**, imposable by the Assessing Officer.
- **Quoting an incorrect TAN** in any challan, statement, certificate or other document attracts a **penalty of ₹10,000 under section 272BB(1A)**.
- **No penalty** is imposed if the person proves **reasonable cause** for the failure (s. 273B) — e.g. a bona fide clerical error — and the person is given an opportunity of being heard.
- **Practical fallout:** banks may **refuse TDS challans/returns** without a valid TAN, and statements filed with a wrong/duplicate TAN cause **mismatch of TDS credit** in the deductees' Form 26AS / AIS, generating grievances and demands.

Legal & procedural references

- **Section 203A**, Income-tax Act, 1961 — requirement to apply for, obtain and quote TAN (and where to quote it — s. 203A(2)).
- **Section 272BB(1) / (1A)** — penalty of ₹10,000 for failure to obtain TAN / for quoting an incorrect TAN.
- **Section 273B** — no penalty where reasonable cause is proved.
- **Rule 114A**, Income-tax Rules, 1962 — application for TAN in **Form 49B**.
- Sections **194-IA / 194-IB / 194M** — deductors exempt from TAN (quote PAN; Forms 26QB/26QC/26QD).
- Sections **192–195, 206C, 200, 201/201(1A)** — TDS/TCS deduction/collection, statements and default context.
- ITBA **TAN Module** — departmental procedure for end-to-end management of the TAN life-cycle (allotment, maintenance, update/closure, restoration, de-duplication, transfer, jurisdiction and intimation).

Key Takeaways

- **TAN** = Tax Deduction and Collection Account Number: a **10-character** code, pattern **4 letters + 5 digits + 1 letter** (AAAA99999A); positions 1–3 = city/jurisdiction code, 4 = initial of deductor's name, 5–9 = serial, 10 = check letter.

- Legal basis = **section 203A**; application = **Form 49B** under **Rule 114A**; allotted via **Protean/NSDL (TIN-FC / online)** or the e-filing portal.
- **Distinguish TAN (AAAA99999A) from PAN (AAAAA9999A)** — different structures, different purpose (deductor vs taxpayer), different sections (203A vs 139A).
- TAN matters because **TDS credit reaches the deductee's Form 26AS/AIS only when the correct TAN is quoted**; for the Department it is the key that tracks each deductor across ITBA, TDS module and TRACES.
- A deductor must hold **only one TAN**; extras are resolved by **de-duplication** — retain one, **Mark Duplicate** and reject the rest.
- Persons deducting under **194-IA, 194-IB, 194M do NOT need TAN** — they quote **PAN** and file Forms **26QB / 26QC / 26QD**.
- **Penalty = ₹10,000 under section 272BB** for not obtaining/quoting TAN or quoting a wrong TAN; waived on **reasonable cause (s. 273B)**.
- ITBA **TAN Module** functions: **Allotment, Maintenance/View, Update & Closure (with Abort), Restoration, Duplicity Resolution, Transfer (incl. across RCC), Jurisdiction Details, Intimation Letter, Life Cycle Summary.**
- **TAN Transfer** proceeds in stages:

1. the **Source AO** initiates the transfer;
2. a **workitem** is created in the worklist; and
3. the **Destination AO approves or rejects** it.

- Cross-RCC transfers can be **re-assigned** from one AO to another (AO1 to AO2).
- TAN is **linked to the deductor's PAN** (one PAN can have several **Linked TANs**) and is **mapped to an AO(TDS)** jurisdiction.

Key terms & abbreviations

- **TAN** — Tax Deduction and Collection Account Number.
- **PAN** — Permanent Account Number (taxpayer identity; linked to TAN in ITBA).
- **TDS / TCS** — Tax Deducted at Source / Tax Collected at Source.
- **AO (TDS)** — Assessing Officer for TDS; jurisdictional authority over deductors.
- **TRACES / CPC-TDS** — TDS Reconciliation Analysis and Correction Enabling System (the TDS Centralised Processing Cell portal).
- **Form 26AS / AIS** — annual tax statement / Annual Information Statement where a deductee's TDS credit appears.
- **TIN-FC** — TIN Facilitation Centre (Protean/NSDL).
- **RCC** — Regional Computer Centre.
- **DDO** — Drawing and Disbursing Officer (a common government deductor).
- **Form 49B** — application form for allotment of TAN (Rule 114A).
- **NOPC** — Nature of Payment / Collection.
- **Workitem** — an ITBA workflow task pending in a user's worklist.

05. TDS Module in ITBA and the CPC-TDS / TRACES Interface

Applicable to: ITO Paper-V, ITI Paper-IV, MS Paper-IV (all three cadres).

Syllabus reference: ITBA Applications Modules — (k) TDS. Administration of Tax Deduction/Collection at Source through ITBA and its interface with CPC-TDS (Ghaziabad) and the TRACES portal.

Overview

Tax Deducted at Source (TDS) and Tax Collected at Source (TCS) are the single largest and most reliable stream of direct-tax collection in India. They are governed by **Chapter XVII-B** (deduction) and **Chapter XVII-BB / s.206C** (collection) of the Income-tax Act, 1961. The system is **deductor/collector-centric**: the person paying the income (not the recipient) obtains a TAN, deducts tax, deposits it into the Government account, files quarterly statements, and issues certificates. The **processing** of these statements and the generation of tax credit (Form 26AS / AIS) is centralised at the **Centralised Processing Cell–TDS (CPC-TDS) at Ghaziabad**, which delivers all deductor/deductee services through the **TRACES** portal. The **ITBA TDS module** is the field officer's (AO-TDS) workbench for the enforcement functions that cannot be centralised — surveys, spot verification, scrutiny, orders u/s 201/201(1A), penalty, prosecution, and verification of foreign remittances (Form 15CA/15CB). This chapter explains the underlying concepts from first principles, then the systems and the officer's workflow.

What TDS is — the "pay-as-you-earn" principle

TDS means that when a specified payment (salary, interest, rent, contract payment, commission, professional fees, etc.) is made, the **payer** deducts a prescribed percentage as income tax **at the moment of payment or credit** and remits it directly to the Government on the recipient's behalf. The recipient receives the net amount; the tax already stands paid against their PAN. This embodies the **"pay-as-you-earn"** (PAYE) idea — tax is collected in small instalments as income arises, rather than in one lump sum after the year ends.

Why it matters to the taxpayer (deductee): the tax deducted is **pre-paid tax / a credit they can set off against their final liability** when filing the return; it spreads the burden over the year and prevents a large year-end payment. If deductions exceed liability, the excess is **refunded**.

Why it matters to the Department: it guarantees a **steady, advance flow of revenue** throughout the year (aiding budget certainty and reducing collection cost), and — equally important — it casts a **wide information net**. Every deduction generates a data trail (who paid whom, how much) that the Department uses to detect income that a recipient might otherwise not disclose. TDS is thus both a collection tool and an information-gathering tool.

Key stakeholders and identifiers

- **Deductor / Collector** — the person responsible for deducting/collecting tax; identified by a **TAN** (Tax Deduction and Collection Account Number, s.203A), a 10-character alphanumeric ID that must be quoted on every challan, statement and certificate. Government deductors who pay tax by book-adjustment (no physical challan) use an **AIN** and file **Form 24G**.
- **Deductee / Collectee** — the person from whose income tax is deducted; identified by **PAN**. Furnishing an invalid PAN or none attracts a **higher deduction under s.206AA**; being a non-filer of returns attracts the higher rate under **s.206AB**.
- **CPC-TDS, Ghaziabad** — the centralised back office that processes all TDS/TCS statements u/s 200A / 206CB and operates TRACES.
- **AO-TDS** — the jurisdictional Assessing Officer (TDS) under a **CIT(TDS)** / Range, who performs enforcement through the **ITBA TDS module**.

The compliance life-cycle — deduct, deposit, report, certify

A deductor's obligations run in four steps, and understanding this cycle is the key to understanding every default the system flags later: 1. **Deduct** the correct amount at the correct rate at the time of payment/credit (whichever is earlier). 2. **Deposit** the tax into Government account by the due date (generally by the **7th of the following month**; different rule for March). 3. **Report** by filing a **quarterly statement** (return) giving deductee-wise, challan-wise details. 4. **Certify** — issue a TDS certificate to each deductee so they can claim the credit. A failure at any step produces a specific consequence: short/late **deduction**, short/late **payment**, late/incorrect **statement**, or non-issue of **certificate** — each with its own interest, fee or penalty discussed below.

TDS/TCS statements (quarterly returns)

Deductors file **quarterly** statements under **s.200(3) and Rule 31A** (TCS under Rule 31AA):

Form	Covers
24Q	TDS on **salaries** (s.192)
26Q	TDS on payments to **residents** other than salary (interest, rent, contract, professional fees, etc.)
27Q	TDS on payments to **non-residents** (s.195 and allied sections)
27EQ	**TCS** statement u/s 206C

Due dates: 31 July (Q1), **31 October** (Q2), **31 January** (Q3) and **31 May** (Q4). The statement is the pivot of the whole system — the credit that ultimately reaches a deductee's 26AS is only as good as the statement the deductor files, so an error in PAN, amount or challan here is what surfaces later as a mismatch.

TDS certificates — Form 16, 16A and 27D

Certificates are issued under **s.203 (TDS) and s.206C(5) (TCS)** and are downloaded from TRACES so that the figure on the certificate always ties to the credit in 26AS: - **Form 16** — the **annual salary** certificate (Part A: tax deducted/deposited from TRACES; Part B: salary computation), issued annually by 15 June following the financial year in which the tax was deducted. - **Form 16A** — the **quarterly** certificate for **non-salary** TDS (26Q/27Q), issued within 15 days of the statement due date. - **Form 16B / 16C / 16D / 16E** — certificates for TDS on **immovable property (194-IA)**, **rent by individuals (194-IB)**, **contractual/professional payments by individuals (194M)** and **virtual digital assets (194S)** respectively. - **Form 27D** — the **TCS** certificate under s.206C.

Why certificates matter: to the taxpayer they are documentary proof of tax paid, needed to claim credit and reconcile with 26AS; to the Department they close the loop — because they are generated only from processed statement data on TRACES, a genuine certificate cannot exist without a matching entry in the Department's records.

Form 26AS and AIS/TIS — the taxpayer's tax information

The Department maintains two PAN-linked information statements the taxpayer relies on: **Form 26AS** (the tax-credit passbook, on TRACES) and the **AIS/TIS** (the wider information net, on the e-filing portal). Their scope and the way errors are corrected differ, as set out below.

Form 26AS — what it is

Form 26AS is the taxpayer's annual consolidated tax statement, maintained against their PAN (originally under Rule 31AB, now under **s.285BB / Rule 114-I**). Think of it as a **"tax passbook"**. Historically it showed TDS, TCS, advance tax, self-assessment tax, refunds and high-value transactions; **from AY 2023-24 the TRACES Form 26AS displays primarily TDS/TCS data**, while the broader financial-transaction information has moved to the AIS (below).

What it contains (TDS/TCS view): deductor-wise entries showing the deductor's **TAN and name**, the **amount paid/credited**, the **tax deducted and deposited**, the section under which it was deducted, and the challan/booking details — plus advance/self-assessment tax paid and refunds during the year.

Why it matters to the taxpayer: it is the **basis for claiming TDS credit**. Credit in the return is allowed by matching against 26AS; a claim not reflected in 26AS is liable to be disallowed under s.143(1). The taxpayer uses 26AS to **verify** that every deduction actually reached the Government under their PAN before they file.

Why it matters to the Department: 26AS is a powerful **cross-verification** tool. It lets the system automatically match the credit a taxpayer claims against the credit the deductor has reported, **reducing evasion and wrong claims** and enabling the CPC to raise or adjust demand under s.143(1) without human intervention.

AIS / TIS versus Form 26AS — what changed and why

The **Annual Information Statement (AIS)** and its condensed companion, the **Taxpayer Information Summary (TIS)**, were introduced on the **e-filing portal (incometax.gov.in)** to widen the information net well beyond tax credits.

- **AIS** consolidates data reported by many sources — banks, mutual funds, registrars, companies, employers, the sub-registrar, GSTN — to show **savings/FD interest, dividends, rent received, securities and property transactions, foreign remittances, GST turnover** and more, alongside the TDS/TCS and tax-payment data. Crucially, AIS is **interactive**: the taxpayer can submit **feedback** ("information is correct / duplicate / relates to other PAN", etc.) on each entry.
- **TIS** is the **category-wise summary** of AIS after de-duplication, showing the *processed value* and the *value accepted*, and is used to **pre-fill** the return.
- **Form 26AS** now focuses on TDS/TCS and tax-payment records.

Why the change: AIS moves the system from merely recording *tax already deducted* to presenting a **360-degree picture of a taxpayer's financial year**, supporting pre-filled returns, e-Verification and nudge-based voluntary compliance. **Practical rule to remember:** *TDS credit is claimed on the basis of Form 26AS, not AIS*; AIS/TIS are primarily for income verification and pre-filling, and errors in AIS are corrected through **feedback**, whereas errors in 26AS are corrected only when the **deductor revises the TDS statement**.

The TRACES portal — what it is and why it matters

TRACES (TDS Reconciliation Analysis and Correction Enabling System) is the CPC-TDS web portal (tdscpc.gov.in) and the single window through which deductors, deductees and the Department transact on TDS. **Why it matters:** it converts raw statement data into usable services and is where every default is displayed and cured. Key facilities: - **Default Summary** — statement-wise list of defaults raised on processing. - **Justification Report** — a detailed, **line-by-line** report explaining each default (short deduction, interest, 234E fee, PAN errors), used by the deductor to understand and correct. - **Consolidated (Conso) File** — the consolidated statement downloaded to prepare a **correction** statement. - **Online correction** — correcting PANs, challans and details without re-filing the full return; **OLTAS challan correction** for challan errors. - **Certificate download** — Form 16/16A/27D. - **Deductee/PAN facilities** — view/verify 26AS, aggregated TDS compliance, and Form 26A/27BA functionality.

Processing under section 200A — how statements are assessed

Every TDS statement is processed **u/s 200A** (TCS statements **u/s 206CB**) by CPC-TDS. On processing, the system: - corrects **arithmetical errors** and **incorrect claims** apparent from the statement; - verifies the **challan** against OLTAS and PANs against the PAN database; - computes **interest** and the **fee u/s 234E**; and - generates an **intimation** to the deductor, which is **deemed a notice of demand under s.156** (so it is appealable and recoverable like any demand).

This is the automated, centralised counterpart of assessment for the TDS world — fast, rule-based, and applied uniformly to every statement filed.

Defaults raised on processing

The defaults visible on TRACES after 200A processing include: - **Short deduction** — tax deducted at less than the correct rate/amount. - **Short payment** — tax deducted but not fully deposited (often a challan mismatch). - **Late deduction interest — s.201(1A)(i): 1% per month** (or part) from the date the tax was **deductible** to the date it was actually **deducted**. - **Late payment interest — s.201(1A)(ii): 1.5% per month** (or part) from the date of **deduction** to the date of **deposit**. - **Late filing fee u/s 234E — ₹200 per day** of delay in filing the statement, **capped at the amount of TDS** in the statement. - **PAN errors** — invalid/"PAN not available" triggering higher-rate demand under s.206AA. - **Challan mismatch** — challan quoted in the statement not matching OLTAS.

Interest and fee provisions — s.234E and s.201/201(1A)

The interest and fee heads flagged during processing are governed by two provisions — the s.234E late-filing fee and the s.201/201(1A) "assessee in default" and interest regime.

Section 234E — the late-filing fee (concept)

s.234E levies a **mandatory fee of ₹200 for every day** the quarterly statement remains unfiled after the due date, subject to a ceiling equal to the total TDS/TCS of that statement. It is a **fee, not a penalty** — it is charged automatically on processing, is not discretionary, and cannot be waived by the AO. It exists to enforce **timely reporting**, because delayed statements delay the credit reaching deductees' 26AS.

Section 201 / 201(1A) — "assessee in default" and interest (concept)

If a deductor **fails to deduct** tax, or deducts but **fails to pay it to the Government, they are treated as an "assessee in default"** under **s.201(1)** and the tax can be recovered from them — even though it was never their own income — **plus interest under s.201(1A)** (1% for non/late deduction, 1.5% for late payment, as above). A humane safeguard exists in the **first proviso to s.201(1)**: where the payee is a resident who has already filed their return**, included the income and paid the tax**, and furnishes an accountant's certificate in **Form 26A**, the deductor is **not** treated as in default for the tax (though **interest** for the intervening period still applies). This prevents double collection of the same tax.

The ITBA TDS module — AO-TDS enforcement

Where CPC-TDS handles the mechanical processing, the **ITBA TDS module** is the AO-TDS's tool for **discretionary enforcement**. ITBA gives the officer a **role-based worklist**; pendency is created automatically as a case/work-item and routed up to the **Range Officer / CIT(TDS)** wherever approval is required.

Core enforcement functions and worklist

Core functions of the AO-TDS through the module: - **Survey u/s 133A** — including **s.133A(2A)**, a survey conducted *specifically to verify TDS compliance* at the deductor's business premises: the officer initiates the proceeding, the system generates a **survey ID**, findings are recorded, and results appear in the initiating user's worklist. - **Spot verification / inspection** of deductor books, ledgers and challans. - **TDS scrutiny** of deductors — selection, issue of notices/letters, and examination of whether tax was correctly deducted, deposited and reported. - **Orders u/s 201(1) / 201(1A)** — formally treating the deductor as an assessee in default and computing tax + interest (subject to the Form 26A proviso). - **Penalty and prosecution** proceedings (below). - **TDS reconciliation** — reconciling OLTAS challans, statements and credit to resolve defaults.

Penalties and prosecution for TDS defaults

- **s.271C** — penalty for **failure to deduct** (or to pay certain tax): a penalty **equal to the amount of tax not deducted/paid**.
- **s.271H** — penalty for **failure to furnish the statement**, or furnishing **incorrect information** in it: **₹10,000 to ₹1,00,000**. *No* penalty is levied if the tax with interest and 234E fee is paid **and** the statement is filed within **one year** of the due date.
- **s.272A(2) — penalty for failure to issue the TDS certificate (or comply with certain notices): ₹500 per day of default (enhanced from ₹100 w.e.f. 01.04.2022).**
- **s.276B** — **prosecution** for **failure to pay** deducted tax to the Government: **rigorous imprisonment of 3 months to 7 years, plus fine**. (Non-deduction is penalised; non-*payment* of tax already deducted is prosecutable, being effectively misappropriation of Government money.) These are imposed by the AO-TDS through ITBA, with statutory opportunity of hearing, and — for prosecution — sanction of the competent authority.

Foreign remittances — Form 15CA / 15CB (ITBA TDS Phase-1)

A headline function of the **ITBA TDS module (Phase-1)** is the **verification of foreign remittances**. Before remitting a sum to a non-resident, the remitter files **Form 15CA** (a self-declaration) and, where required, obtains a chartered accountant's certificate in **Form 15CB**, under **s.195(6) and Rule 37BB**. This ensures that any **TDS under s.195** on the foreign payment is captured *before* money leaves the country.

In ITBA the officer's workflow is: - **View Form 15CA** filed by the remitter. - Examine the remittance under the **Section-B tabs — Remittance, IT Act, DTAA and TDS** — to see the nature of payment, the Act provision applied, any treaty (DTAA) relief claimed, and the TDS deducted. - **Flag** remitter transactions and, via the **"Yes" hyperlink in the Flagged column**, drill into **Remitter Transaction details**. - Record verification against each transaction — **Useful (Yes/No), Remarks, Result** — and click **Verify**. - **Generate Letter** to the assessee to call for further information. - **Propose for Closure** to the **Range Officer** (e.g. where the verification is nil or the remittance is within the prescribed threshold), routing the case up for approval.

This links the AO-TDS enforcement role directly with **s.195 TDS on non-resident payments** and treaty administration.

Worked example (tying the concepts together)

A company deducts ₹1,00,000 TDS on interest in June (Q1) but deposits it in September and files 24Q/26Q on 30 September instead of 31 July. On 200A processing CPC-TDS will raise: **late-payment interest** at 1.5% p.m. under s.201(1A)(ii) for the months of delay; a **234E fee** of ₹200 × days late (capped at ₹1,00,000); and an **intimation** (deemed s.156 demand) on TRACES. Meanwhile the deductees' 26AS credit is delayed until the statement is filed. The deductor cures it by paying the demand and, if any PAN was wrong, filing an **online correction** using the **Conso File**. If facts suggest wilful default, the **AO-TDS** may proceed under **s.271H / 276B** through ITBA.

Legal & procedural references

- **Chapter XVII-B / XVII-BB**, Income-tax Act, 1961 (deduction/collection at source); **s.206C** (TCS).
- **s.200 / 200A** — duty to deposit and file statements / processing of TDS statements; **s.206CB** (TCS processing).
- **s.201(1) & 201(1A)** — assessee in default; interest @ 1% (non/late deduction) and 1.5% (late payment) p.m.; first proviso + **Form 26A**.
- **s.203 / 203A / 203AA (omitted w.e.f. 01.06.2020; see s.285BB), Rules 31, 31A, 31AA, 114-I (formerly 31AB), 37BB** — certificates, TAN, 26AS, Form 15CA/CB.

- **s.234E** — late-filing fee ₹200/day (capped at TDS); **s.271C, 271H, 272A(2)** — penalties; **s.276B** — prosecution.
- **s.133A / 133A(2A)** — survey; **s.156** — notice of demand (a 200A intimation is deemed such notice).
- **s.195 / 195(6)**, **s.206AA, 206AB**, **s.285BB** (Form 26AS/AIS); **CPC-TDS, Ghaziabad**; **TRACES** portal.

Key Takeaways

- TDS is India's **pay-as-you-earn** mechanism: the payer deducts and remits tax; to the deductee it is **pre-paid credit**, to the Department it is **steady revenue plus a wide information net**.
- Compliance has four steps — **deduct, deposit, report (quarterly statement), certify** — and every default (short/late deduction or payment, late statement, no certificate) maps to one of these.
- **Statements:** 24Q (salary), 26Q (resident non-salary), 27Q (non-resident), 27EQ (TCS). Due dates **31 Jul / 31 Oct / 31 Jan** and **31 May** for Q4.
- **Form 26AS** is the taxpayer's tax passbook (now mainly TDS/TCS); **TDS credit is claimed on the basis of 26AS**, and it lets the Department **cross-verify** claims against deductor reporting.
- **AIS** widens the net (interest, dividends, rent, property, remittances, GST turnover) with taxpayer **feedback**; **TIS** summarises AIS to **pre-fill** returns. AIS errors are fixed by feedback; 26AS errors only by the deductor revising the statement.
- All statements are **processed u/s 200A (TCS: 206CB) by CPC-TDS Ghaziabad**; the intimation is a **deemed notice of demand u/s 156**. Everything is serviced on **TRACES** (Justification Report, Conso File, Default Summary, certificate download).
- **s.201(1A):** interest **1% p.m.** for non/late deduction, **1.5% p.m.** for late payment; deductor is not "in default" for tax if payee-side compliance is proved via **Form 26A** (interest still applies).
- **s.234E:** ₹200/day fee, capped at TDS — automatic, non-waivable. **s.271H:** ₹10,000–1,00,000 (waived if cured within one year). **s.271C:** penalty = tax not deducted. **s.276B:** RI **3 months–7 years** for not paying deducted tax.
- The **ITBA TDS module** is the AO-TDS workbench for what CPC cannot centralise: **surveys u/s 133A/133A(2A)**, spot verification, scrutiny, orders u/s **201/201(1A)**, penalty and prosecution, all via a **role-based worklist** routed to the Range/CIT(TDS).
- **ITBA TDS Phase-1** centres on **foreign-remittance verification**: View **Form 15CA**, examine **Section-B tabs (Remittance / IT Act / DTAA / TDS)**, record **Useful/Remarks/Result**, **Generate Letter**, and **Propose for Closure** to the Range Officer (s.195 / Rule 37BB).

Key terms & abbreviations

- **TDS / TCS** — Tax Deducted / Collected at Source.
- **TAN / AIN / PAN** — Tax Deduction & Collection A/c No. / Accounts Office Identification No. / Permanent Account No.
- **CPC-TDS** — Centralised Processing Cell–TDS, Ghaziabad.
- **TRACES** — TDS Reconciliation Analysis and Correction Enabling System.
- **AO-TDS / CIT(TDS)** — Assessing Officer / Commissioner handling TDS jurisdiction.
- **26AS / AIS / TIS** — annual tax-credit statement / annual information statement / taxpayer information summary.
- **OLTAS** — On-Line Tax Accounting System (challan data).

- **Form 26A** — accountant's certificate saving a deductor from "assessee in default" status (proviso to s.201(1)).
- **Form 15CA / 15CB** — remitter declaration / CA certificate for foreign remittances (s.195(6), Rule 37BB).
- **Form 24G** — monthly statement by Government (book-entry) deductors filed under an AIN.
- **Justification Report / Conso File** — TRACES default-detail report / consolidated statement for corrections.

Part III — Returns, Assessment & Faceless Assessment

06. ITR Processing and CPC-ITR

Applicable to: ITO Paper-V, ITI Paper-IV, MS Paper-IV (all three cadres).

Syllabus reference: ITBA Applications Modules — ITR processing (e-filing & e-verification; pre-filling; processing u/s 143(1); CPC-ITR; defective returns; refunds and adjustments; AO interaction with CPC).

Overview

Almost every income-tax return (ITR) in India is now filed **electronically** on the **e-Filing portal** (incometax.gov.in) and processed in **bulk** by the **Centralised Processing Centre for Income-Tax Returns (CPC-ITR), Bengaluru**, under **section 143(1)** of the Income-tax Act, 1961. CPC performs an automated **"summary assessment"** — it validates the return, makes only the limited **prima facie adjustments** the law permits, computes tax/interest, determines any refund or demand, and issues an **intimation u/s 143(1)**. The field **Assessing Officer (AO)** does not process the bulk of returns; the AO comes in for **scrutiny (143(2))**, **rectification (154)**, **grievances**, and **defective-return (139(9))** handling. This chapter develops the topic from first principles — what a return is, the Rule-12 forms, pre-filling, e-verification, 143(1) processing, refunds and set-off, and the AO–CPC interface.

The end-to-end pipeline

The processing pipeline proceeds through the following stages, each of which is examined in turn below: 1. **File** the return on the e-Filing portal (pre-filled). 2. **e-Verify** the return within 30 days. 3. **CPC validation** of the verified return. 4. **Processing u/s 143(1)**, with only the permissible prima facie adjustments. 5. **Intimation** of the result — refund, demand, or no-change. 6. **Optional set-off** of any refund against an outstanding demand u/s 245. 7. **Downstream AO functions**, where applicable — 143(2) scrutiny, 154 rectification, and 139(9) defect handling.

The income-tax return, the filing obligation and Rule 12 forms

What an income-tax return (ITR) is — and why filing matters

What it is. An income-tax return is a **statement furnished to the Department by a taxpayer** declaring, for a **previous year**, the total income earned, the deductions/exemptions claimed, the tax computed thereon, and the taxes already paid (TDS, TCS, advance tax, self-assessment tax). The legal duty to furnish a return flows from **section 139**. Filing is done on the e-Filing portal in the form prescribed by **Rule 12**.

Why it matters — to the taxpayer. The return is the taxpayer's **self-assessment**: it is how one discloses income, claims **refunds** of excess tax, carries forward **losses** (allowed only if the return is filed by the due date u/s 139(1)), and creates a documented income record needed for loans, visas and capital-gains proof. Filing on time avoids **late-filing fee u/s 234F** and **interest u/s 234A**.

Why it matters — to the Department. The return is the **primary input** to the entire assessment machinery. It is the document processed u/s 143(1), matched against third-party data (26AS/AIS), risk-scored for scrutiny (CASS), and used to determine collection and refund. Voluntary, accurate, timely returns are the backbone of a self-assessment tax system, minimising the need for intrusive enforcement.

Who must file — the filing obligation

Filing is **mandatory** for persons whose total income exceeds the basic exemption limit, and for companies and firms **irrespective of income**. It is also mandatory in certain "high-value transaction" situations even where income is below the threshold (e.g., large deposits, foreign travel spend, electricity bills, sales turnover thresholds). Others file voluntarily to claim refunds. The **form** to be used, and the **manner** (electronically, with or without DSC), are dictated by **Rule 12**.

The ITR forms under Rule 12 — what they are and why they differ

What it is. Rule 12 of the Income-tax Rules, 1962, is the rule that prescribes **which ITR form** applies to whom and the **manner** of furnishing it. There are seven notified forms; the correct one depends on the taxpayer's **status** (individual/HUF/firm/company/trust) and the **nature of income** (salary, house property, business, capital gains, etc.).

Why it matters. Filing the **wrong form** can render a return **defective u/s 139(9)**. Matching income type to form also lets CPC apply the right validations automatically.

Form	Broadly for (AY 2025-26)
ITR-1 (Sahaj)	Resident individual, total income ≤ ₹50 lakh — salary, one house property, other sources; **now also LTCG u/s 112A up to ₹1.25 lakh** (no capital-loss carry-forward).
ITR-2	Individuals/HUFs with **no business/profession** income (capital gains, more than one house, foreign assets/income, director/unlisted shares, etc.).
ITR-3	Individuals/HUFs having **income from business or profession**.
ITR-4 (Sugam)	Resident individual/HUF/firm (non-LLP) opting for **presumptive** income u/s 44AD/44ADA/44AE, income ≤ ₹50 lakh; also LTCG u/s 112A up to ₹1.25 lakh.
ITR-5	Firms, LLPs, AOPs, BOIs, and similar entities.
ITR-6	Companies (other than those claiming exemption u/s 11).
ITR-7	Trusts/charities and others filing u/s 139(4A)–(4F).

What changed for AY 2025-26

The most notable change: **small investors** with **LTCG u/s 112A up to ₹1.25 lakh** (from STT-paid listed equity shares / equity mutual funds) may now report it in the **simpler ITR-1 / ITR-4**, provided there is **no brought-forward or carried-forward capital loss**. Earlier such taxpayers were forced into ITR-2/ITR-3. This eases compliance for a very large class of salaried small investors.

Belated, revised and updated returns — sections 139(4), 139(5) and 139(8A)

Belated and revised returns — sections 139(4) and 139(5)

- **Belated return u/s 139(4):** filed after the due date u/s 139(1) but at any time before three months prior to the end of the relevant assessment year (i.e., by 31 December of the AY) or before completion of the assessment, whichever is earlier; attracts **234F fee** and **234A interest**, and **bars carry-forward** of most losses.
- **Revised return u/s 139(5):** filed to **correct an omission or wrong statement** in an original/belated return, within the same window. A revised return **replaces** the earlier one for processing.

Updated return u/s 139(8A) (ITR-U) — awareness

What it is. The **updated return (ITR-U)**, introduced by the Finance Act 2022, lets a taxpayer **voluntarily disclose additional income** and pay the resulting tax **after** the normal due dates — a compliance-encouraging window. It can be used **only to increase income/tax**; it **cannot** be filed to **reduce income, claim/increase a refund, or report/increase a loss**.

Position for AY 2025-26. The window was **24 months** from the end of the relevant assessment year, with **additional tax** of **25%** (if filed within 12 months) or **50%** (if filed in the 13th–24th month) of the aggregate of tax and interest.

Awareness — later widening. The **Finance Act 2025** extended the window to **48 months** and added slabs of **60%** (3rd year) and **70%** (4th year) additional tax, with restrictions where a notice u/s 148A has issued. Candidates should be **aware** of this extension while noting that the FY 2024-25/AY 2025-26 baseline is the 24-month/25%–50% position.

What CPC-ITR (Bengaluru) is — and why centralised processing matters

What it is. CPC-ITR is the **Centralised Processing Centre for Income-Tax Returns** at **Bengaluru**, established under **section 143(1A)** and the CBDT's **Centralised Processing of Returns Scheme**. It is a **technology-driven back office** that receives every e-filed, e-verified return and processes it **in bulk, without any interface** with the taxpayer or the jurisdictional AO. (It is distinct from the Centralised Processing Cell-TDS (CPC-TDS), which processes TDS statements through TRACES.)

Why centralised processing matters — to the taxpayer. Speed and predictability. Returns are processed and refunds issued in days/weeks rather than through slow, officer-by-officer manual processing. Rules are applied **uniformly**, so identical returns are treated identically regardless of location.

Why it matters — to the Department. Scale, uniformity, and freeing up officers. CPC handles crores of returns automatically, applies consistent validations and adjustments, curbs discretion-driven errors, and lets field officers concentrate on **scrutiny and enforcement** rather than routine data processing. It also feeds clean, structured data into **CASS/Insight** for risk assessment.

Pre-filling and the underlying data statements

What it is. Pre-filling means the e-Filing utility **auto-populates** the return with data the Department already holds — personal details, salary from **Form 16**, interest/other income, and **tax credits** — drawn from **Form 26AS**, the **AIS/TIS**, and TDS certificates. The taxpayer **reconciles** these figures against personal records before submitting.

Why it matters — to the taxpayer. Ease and accuracy. Less manual data entry, fewer keying errors, and a ready reconciliation of what the Department already knows, reducing the chance of a mismatch notice.

Why it matters — to the Department. Pre-filled data that matches the return means **fewer 143(1)(a) adjustments and notices**, cleaner processing, and a strong deterrent against under-reporting (the taxpayer sees the Department already has the third-party figures).

Form 26AS — the tax-credit statement

What it is. A consolidated **annual tax statement** (available via TRACES/e-Filing) showing **TDS/TCS credited**, advance/self-assessment tax paid, and certain high-value transactions against the taxpayer's PAN. **Why it matters:** it is the primary proof of **taxes paid**; refunds and demand hinge on matching return figures to 26AS credits.

AIS and TIS — the wider information view

What it is. The **Annual Information Statement (AIS)** is a comprehensive statement of the taxpayer's financial information (interest, dividends, securities/mutual-fund transactions, foreign remittances, SFT data) sourced through **Project Insight**; the **Taxpayer Information Summary (TIS)** is its aggregated, category-wise summary that feeds pre-filling. **Why it matters:** AIS lets the taxpayer report completely and gives the Department a 360° view to detect omissions — including **143(1)(a)(vi)** additions.

Form 16 / Form 16A — TDS certificates

What it is. Form 16 is the employer's **TDS certificate on salary**; **Form 16A** covers TDS on non-salary payments. **Why it matters:** they are the taxpayer's evidence of income and tax deducted, and their figures must reconcile with 26AS and the return.

e-Verification — what it is and why an unverified return is invalid

What it is. e-Verification is the step that **authenticates** that the return was genuinely filed by the taxpayer. A filed return is **not a valid return until verified** — an unverified return is treated as if **never furnished**.

Why it matters — to the taxpayer. Verification is what makes the return legally effective and triggers processing/refund. Miss it and losses, refunds and the return itself lapse.

Why it matters — to the Department. It provides **authentication and non-repudiation** without paper, letting a fully digital pipeline run at scale.

The 30-day window

Verification must be completed **within 30 days** of transmitting the return data. The date on which verification is completed (or the signed **ITR-V** is **received at CPC**) governs validity; verify late and the return is treated as filed on the **date of verification** (with belated-filing consequences).

Modes of verification

- **Aadhaar OTP** — one-time password to the Aadhaar-registered mobile.
- **EVC (Electronic Verification Code)** — generated via net-banking, a **pre-validated** bank account, demat account, or bank ATM.
- **DSC (Digital Signature Certificate)** — **mandatory** where accounts are subject to audit (companies, tax-audit cases, etc.).
- **ITR-V** — the physical, signed one-page **acknowledgement**; where e-verification is not used, ITR-V is sent by **ordinary/speed post** to **Centralised Processing Centre, Income Tax Department, Bengaluru – 560500** within the 30-day window. CPC acknowledges receipt, and only then is the return taken up for processing.

Processing u/s 143(1) and the prima facie adjustments

What it is. Section **143(1)** mandates a **centralised, automated** processing of **every valid return**. It is a **summary assessment**, not a scrutiny: CPC does not examine the merits or call for evidence. It computes total income/loss after making **only** the limited **prima facie adjustments** the law allows, then computes tax, interest and fee, and arrives at a **refund, demand, or no-change**.

Why it matters. For the vast majority of taxpayers, **143(1) is the only "assessment" their return ever sees** — it is what releases the refund or raises the demand. Understanding its narrow scope explains why CPC **cannot** decide debatable questions.

The six prima facie adjustments u/s 143(1)(a)

Total income is adjusted **only** for these six clauses — apparent errors evident from the return and information already with the Department:

1. **143(1)(a)(i)** — any **arithmetical error** in the return.
2. **143(1)(a)(ii)** — an **incorrect claim** apparent from information in the return (e.g., a deduction exceeding a statutory limit, or an entry inconsistent with another entry).
3. **143(1)(a)(iii)** — **disallowance of loss** claimed for set-off where the earlier year's return was filed **beyond the due date** u/s 139(1).
4. **143(1)(a)(iv)** — **disallowance of expenditure / increase in income** indicated in the **audit report** but not taken into account in the return.
5. **143(1)(a)(v)** — **disallowance of deductions** u/s 10AA or Chapter VI-A (80-IA, 80-IAB, 80-IB, 80-IC, 80-ID, 80-IE) where the **return is furnished beyond the due date** u/s 139(1).

6. **143(1)(a)(vi)** — **addition of income** appearing in **Form 26AS / Form 16A / Form 16** that has **not been included** in computing total income.

Debatable issues cannot be adjusted u/s 143(1). The adjustment must be a clear, apparent error — anything requiring interpretation or evidence belongs to scrutiny (143(3)), not summary processing.

The proposed-adjustment notice and the 30-day opportunity

Before making **any** 143(1)(a) adjustment, CPC must give the taxpayer a **prior intimation electronically** (a **proposed-adjustment notice u/s 143(1)(a)**), setting out the adjustment and inviting a response. If **no response** is received within **30 days**, the proposed adjustment is made. This is a **natural-justice safeguard** built into an otherwise automated process.

Intimation u/s 143(1) — output, time-limits, interest and fee

What it is. The **intimation u/s 143(1)** is the **computer-generated communication** that reports the result of processing. It is **password-protected** (PAN in lower case + date of birth), sent to the taxpayer's registered e-mail and e-Filing account, and shows the figures **as filed** side-by-side with **CPC's computed figures**, ending in a **refund, demand, or "no change"**.

Why it matters. It is treated as an **order** for the purpose of **rectification u/s 154**, and where it creates a demand or reduces a refund it can be appealed to the **CIT(A)**. A demand raised by it is recoverable u/s 156.

The 9-month time-limit and deemed intimation

- **Time-limit:** the intimation may be sent **up to 9 months from the end of the financial year in which the return is furnished**. Example: a return filed during **FY 2025-26** can be processed/intimated up to **31 December 2026**.
- **Deemed intimation:** if the period lapses with **no adjustment** and no intimation, the **acknowledgement** of the return is deemed to be the intimation u/s 143(1) — the return is accepted as filed.

Interest and fee reflected in processing

CPC computes, as part of 143(1): **interest u/s 234A** (default in furnishing return), **234B** (default in payment of advance tax), **234C** (deferment of advance-tax instalments), and **late-filing fee u/s 234F** (up to ₹5,000; ₹1,000 where total income ≤ ₹5 lakh). These appear in the intimation and affect the net refund/demand.

Refunds and set-off — sections 244A and 245

Refund determination and interest u/s 244A

Where processing shows **taxes paid exceed the tax due**, CPC determines a **refund** and credits it **directly** to the taxpayer's **pre-validated, PAN-linked bank account** (refunds are not issued to non-validated accounts). **Interest on the refund is allowed u/s 244A, generally from 1st April of the assessment year (or from the date of payment of tax, as applicable) to the date of grant of refund.** This automated, direct-to-bank refund is one of the most visible benefits of centralised processing.

Set-off of refund against demand u/s 245 — what it is and why the safeguard matters

What it is. Section 245 lets the Department **adjust a refund** due to a taxpayer against any **outstanding tax demand** of that taxpayer. But before doing so, it must give the taxpayer a **prior intimation u/s 245** of the proposed set-off and an opportunity (generally **30 days**) to respond.

Why it matters — to the taxpayer. It protects against a refund being silently swallowed by a **wrong or disputed** demand; the taxpayer can object, and if the demand is incorrect the AO must verify/correct it before any adjustment.

Why it matters — to the Department. It is an efficient **recovery** tool — genuine arrears are cleared out of refunds otherwise payable — while the prior-intimation requirement keeps the process fair and legally sound. Only after this is the refund set off and the **balance** released.

Defective returns, rectification and condonation — sections 139(9), 154 and 119(2)(b)

Defective return u/s 139(9)

What it is. A return is **defective** if it is **incomplete or inconsistent** — e.g., required schedules/annexures not filled, tax payable per the return not paid, statements of accounts missing, or a wrong form used.

Process. CPC (or the AO) issues a **defective-return notice u/s 139(9)** giving the taxpayer **15 days** (extendable on application) to **rectify** the defect. If the defect is **not cured** in time, the return is treated as **invalid** — as if **no return had been furnished** — with consequences including **loss of loss carry-forward**, interest/fee, and possible best-judgment assessment.

Rectification u/s 154

What it is. Section **154** allows correction of a **"mistake apparent from the record"** in an order/intimation — e.g., wrong **TDS/26AS credit**, advance-tax/self-assessment-tax mismatch, or an arithmetical slip in the 143(1) intimation.

Where it lies. Immediately after processing, the rectification right rests with **CPC** (the online **"Rectification"** service on the e-Filing portal). Once the record is transferred to jurisdiction, the **AO** rectifies through the **Rectification** module in **ITBA**, passing a 154 order that gives the correct credit/relief. (See Chapter 10 for the full s.154 scheme, including the time-limits.)

Condonation of delay — section 119(2)(b)

Where a return or refund claim is **time-barred**, the taxpayer may seek **condonation of delay** from the prescribed authority (Pr.CIT/CIT/CBDT, depending on the refund amount and monetary limits set by CBDT). If condoned, the belated return/claim can be processed and the refund considered on merits.

Scrutiny selection and the AO–CPC interface

Scrutiny selection — section 143(2), CASS and faceless assessment

Only a **small fraction** of returns are picked for detailed examination. Returns are risk-scored through **CASS (Computer Assisted Scrutiny Selection)** or fall under **compulsory-manual** criteria; selected cases are pushed to the **faceless/jurisdictional AO**, who issues the **notice u/s 143(2)**. That notice must be served **within 3 months from the end of the FY in which the return is furnished**. The assessment that follows is largely **faceless u/s 144B**, conducted through the **Assessment** module of ITBA. Processing u/s 143(1) and scrutiny u/s 143(2) are **parallel tracks** — a return can be processed by CPC and still be selected for scrutiny.

How ITBA officers interact with CPC processing

The field officer's role begins largely **after** CPC processing: - **Scrutiny / transfer u/s 143(2):** CASS-flagged returns are pushed from CPC to the **faceless/jurisdictional AO**, who issues the 143(2) notice and assesses (largely faceless u/s 144B) via ITBA's **Assessment** module. - **Rectification u/s 154:** the AO corrects mistakes in CPC intimations (credit mismatches, arithmetic) through ITBA's **Rectification** module once the record is with jurisdiction. - **Grievances & demand management:** AOs verify/correct outstanding demands ("Response to Outstanding Demand") that feed the **245 set-off** process, and respond to taxpayer grievances (e-Nivaran/CPGRAMS). - **ITR Processing module:** gives the AO **visibility** of CPC-processed returns and lets the AO take up returns **not** processed centrally or routed to jurisdiction.

Legal & procedural references

- **Income-tax Act, 1961:** s. **139** (return), **139(1)** (due date), **139(4)/(5)** (belated/revised), **139(8A)** (updated return), **139(9)** (defective return); **143(1)** & **143(1)(a)(i)–(vi)** (processing/adjustments), **143(1A)** (CPC scheme), **143(2)** (scrutiny notice); **144B** (faceless assessment); **154** (rectification); **156** (notice of demand); **234A/B/C** (interest), **234F** (late-filing fee), **244A** (interest on refund), **245** (set-off of refund against demand); **119(2)(b)** (condonation); **140B** (tax on updated return).
- **Income-tax Rules, 1962: Rule 12** (ITR forms & manner of furnishing).
- **Schemes/Systems:** Centralised Processing of Returns Scheme; **CPC-ITR, Bengaluru**; e-Filing portal (incometax.gov.in); **AIS/TIS** (Project Insight); **Form 26AS** (TRACES); **CASS** (scrutiny selection); **ITBA** modules (ITR Processing, Assessment, Rectification).

Key Takeaways

- **CPC-ITR is at Bengaluru** and does **centralised, automated summary processing u/s 143(1)**; the AO does **not** process the bulk of returns — centralisation buys **speed and uniformity**.
- **Rule 12** prescribes the seven ITR forms; **ITR-1 (Sahaj)** and **ITR-4 (Sugam)** are the simplest (income ≤ ₹50 lakh) and from **AY 2025-26** may include **LTCG u/s 112A up to ₹1.25 lakh** (no capital-loss carry-forward).
- A return is **invalid until verified**; **e-verify within 30 days** via **Aadhaar OTP / EVC / DSC**, else post **ITR-V to CPC Bengaluru – 560500**; the date verification reaches CPC counts.
- **Pre-filling** from **Form 16 / 26AS / AIS-TIS** eases filing for the taxpayer and cuts mismatches for the Department; unreported 26AS income drives **143(1)(a)(vi)** additions.
- **143(1)(a)** allows only **six prima facie adjustments**; **debatable issues cannot be adjusted**; a **30-day proposed-adjustment notice** must precede any adjustment.
- The **intimation u/s 143(1)** shows filed vs computed figures and can be sent **up to 9 months from the end of the FY in which the return is filed**; if none and no adjustment, the **acknowledgement is the deemed intimation**.
- **Refunds** go only to **pre-validated PAN-linked bank accounts**, with **interest u/s 244A**.
- **Section 245** requires **prior intimation (≈30 days)** before a refund is set off against an outstanding demand.
- **Defective return u/s 139(9) → 15 days** to cure, else the return is **invalid** (loss of carry-forward, etc.).
- **143(2) scrutiny notice** must issue within **3 months from the end of the FY**; selection is via **CASS**, assessment largely **faceless u/s 144B** — a track **parallel** to 143(1).
- **Updated return u/s 139(8A)**: for **AY 2025-26**, **24 months** window, **25%/50%** additional tax; be **aware** the Finance Act 2025 extended it to **48 months** (adding 60%/70% slabs).

Key terms & abbreviations

- **CPC-ITR** — Centralised Processing Centre, Income-Tax Returns, Bengaluru
- **ITR / ITR-V** — Income Tax Return / Income Tax Return-Verification (acknowledgement)
- **e-Verification / EVC** — electronic verification / Electronic Verification Code
- **DSC** — Digital Signature Certificate; **OTP** — One-Time Password
- **143(1) intimation** — automated processing communication (refund/demand/no-change)
- **Prima facie adjustment** — limited correction of apparent errors u/s 143(1)(a)
- **AIS / TIS** — Annual Information Statement / Taxpayer Information Summary (Insight)

- **26AS** — annual tax-credit statement (TRACES); **Form 16/16A** — TDS certificates
- **CASS** — Computer Assisted Scrutiny Selection
- **ITR-U** — Updated Return u/s 139(8A); **140B** — tax on updated return
- **234A/B/C, 234F, 244A** — interest/fee/refund-interest provisions
- **AO** — Assessing Officer; **CBDT** — Central Board of Direct Taxes; **ITBA** — Income Tax Business Application

07. Assessment Module in ITBA (Non-Faceless)

Applicable to: ITO Paper-V, ITI Paper-IV. (NOT MS Paper-IV.)

Syllabus reference: Assessment Module (Faceless and non-Faceless) in ITBA — overview; features & functions; selection of cases & notice generation; cancellation of cases selected; Scrutiny Assessment (issuing notice, reference to TPO/VO, additions/disallowances, sending data to CPC-ITR for computation, capturing feedback, passing of Assessment Order); Manual order upload; Set aside cases for fresh assessment to AO; Set aside cases to CIT(A). *(This chapter covers the NON-faceless workflow only; Faceless Assessment u/s 144B is Chapter 08.)*

Overview

The **Assessment module** of the **Income Tax Business Application (ITBA)** is the software through which a **jurisdictional Assessing Officer (AO)** runs the entire scrutiny lifecycle on the departmental network — from **selection of a case** through to the **passing and serving of the Assessment Order** — without leaving the system. This chapter first sets out *what assessment is*, the *different kinds* of assessment, and the key systems and references an AO relies on (**CASS**, **e-Proceedings**, **TPO**, **VO**, **DRP**), so that the concepts are clear before the procedural steps are described; a firm grasp of the concepts makes the workflow considerably easier to follow. The module is integrated with **CASS** (case selection), **e-Filing** (e-Proceedings), **CPC-ITR** (tax computation & matching), and the downstream **Penalty/Demand** modules. This chapter describes only the **non-faceless** (named-AO) flow, where the case sits with a specific AO/Range/PCIT rather than the National Faceless Assessment Centre. The stated learning objective is "to understand the complete flow of Assessment Proceedings from Selection of Case to Passing of Order."

What "assessment" means — and why it matters

An **assessment** is the process by which the Department examines a taxpayer's **return of income**, determines the **correct total income** and the **tax payable (or refund due)**, and records that determination in a formal **assessment order**. In simple terms: the taxpayer *self-declares* income when filing the return; assessment is the Department *checking and, where necessary, correcting* that declaration.

- **Why it matters to the taxpayer:** it converts a self-declaration into a legally settled tax liability, and creates appeal rights. A correct, well-reasoned order protects a genuine taxpayer from unjustified demands.
- **Why it matters to the Department:** assessment is the core enforcement tool for detecting under-reporting/evasion, safeguarding revenue, and creating an audit trail. ITBA makes the whole process **uniform, time-stamped and limitation-aware** across the country.

The types of assessment

Understanding the *statutory categories* of assessment is the foundation of this chapter.

Summary assessment / intimation — s.143(1)

Every return filed is **processed at CPC-ITR** by computer: arithmetic errors, internal inconsistencies, incorrect claims apparent from the return, and TDS/tax-credit mismatches are auto-adjusted, and an **intimation u/s 143(1)** is issued. It is **not** a scrutiny — no officer examines the case; it is machine processing. This is the *default* treatment of a return.

Scrutiny assessment — s.143(3)

A **detailed examination** of the return by an AO, done only in cases *selected* for scrutiny. The AO issues notices, calls for evidence, hears the assessee and passes a **regular assessment order u/s 143(3)**. This is the workflow that the ITBA Assessment module is built around.

Best-judgment assessment — s.144

Where the assessee **fails to file a return**, **fails to comply** with a s.142(1)/143(2) notice, or does not cooperate, the AO may complete the assessment to the **best of their judgment** on the material available (still after giving a show-cause opportunity). In ITBA this is done by **"converting the case to s.144."**

Reassessment / income escaping assessment — s.147 (with s.148/148A)

Where the AO has **information suggesting income has escaped assessment**, the case can be **reopened** under s.147. Since the Finance Act 2021, a mandatory pre-notice procedure under **s.148A** applies (see its own subtopic), after which a **notice u/s 148** is issued and the reassessment is completed. Search/requisition cases use s.153A/153C-type provisions.

> **Illustration.** A salaried taxpayer files a return; CPC issues a 143(1) intimation (summary). CASS later flags a large unexplained deduction, so the case goes into **143(3) scrutiny**. If the same person had never filed and ignored notices, the AO would finalise it under **144**. If, two years after a completed assessment, AIS shows an undisclosed property sale, the AO reopens under **147/148A → 148**.

Case selection (CASS) and electronic proceedings (e-Proceedings)

Two systems underpin the whole non-faceless workflow: **CASS**, which chooses the cases, and **e-Proceedings**, which carries the paperwork online.

What CASS is — and why computer-based selection matters

CASS (Computer Assisted Scrutiny Selection) is the CBDT's system that **selects returns for scrutiny automatically**, using a computer algorithm rather than an officer's discretion. Returns are scored against **objective risk parameters** — e.g. large refund claims, high deductions/exemptions, a sharp fall in gross/net profit, international transactions, expenditure disproportionate to turnover, stock mismatches, or transactions with non-filers — and the risky ones are picked.

- **What it is:** the primary, rule-based engine for choosing scrutiny cases (currently the large majority of scrutiny selections). CASS produces two types — **Limited Scrutiny** (examine only the specific flagged issue) and **Complete Scrutiny** (examine the whole return).
- **Why it matters — objectivity:** because selection is done by machine against uniform parameters, it removes officer discretion and the perception of harassment/favouritism, spreads scrutiny fairly, and lets the Department focus manpower on genuinely risky returns. The parameters are reviewed and refined every year. **Compulsory manual** selection (on CBDT-notified criteria) runs alongside CASS for defined categories.
- In ITBA, CASS cases flow **straight into the "Generate Notice to Initiate Proceedings" screen** — the AO does not select them manually.

What e-Proceedings is — and why it matters

e-Proceedings is the electronic bridge that lets an assessment be conducted **online**, through the taxpayer's **e-Filing account**, instead of by physical visits and paper.

- **What it is:** notices, letters, questionnaires and orders generated in ITBA appear in the assessee's **e-Filing → e-Proceedings** tab; the assessee's **responses and attachments flow back** into the AO's Case History/Notings. The taxpayer can **opt in/opt out**, and the AO can **block/re-enable** response submission. It is enabled for Assessment, e-Nivaran, Exemption, Penalty and Appeal modules.
- **Why it matters:** for the taxpayer — no office visits, a complete online record, response at one's convenience. For the Department — faster service, a tamper-evident audit trail, and it is the technical backbone that made **faceless** working possible.

Specialist references — the TPO (s.92CA) and the Valuation Officer (s.142A)

For technically specialised issues, the AO can hand determination to a dedicated officer.

Reference to the TPO — s.92CA (what & why)

The **Transfer Pricing Officer (TPO)** is a specialist officer who determines the **Arm's Length Price (ALP)** of an assessee's **international transactions** (and specified domestic transactions) with associated enterprises.

- **What it is:** where transfer-pricing issues arise, the AO **refers** the ALP determination to the TPO u/s **92CA** (with prior approval of the PCIT/CIT). The TPO's order on ALP is **binding** on the AO for computing the transfer-pricing addition.
- **Why it matters:** transfer pricing is technically complex; a dedicated officer ensures consistent, expert determination and protects the tax base against profit-shifting. In ITBA the reference **creates a TPO pendency and extends the AO's limitation date.**

Reference to the Valuation Officer — s.142A (what & why)

The **Valuation Officer (VO)** is a departmental valuation expert (Departmental Valuation Officer) who estimates the **fair value/cost** of an asset, investment or property.

- **What it is:** under **s.142A** the AO may refer valuation of any asset/property/investment to the VO; the VO furnishes a **Valuation Report** the AO can use (e.g. for unexplained investment additions).
- **Why it matters:** it gives the AO an independent, defensible valuation instead of a subjective estimate. In ITBA, recording the reference/report **extends the limitation date.**

The DRP — s.144C (what & why)

The **Dispute Resolution Panel (DRP)** is a **collegium of three PCsIT/CsIT** that resolves disputes **before** a final order is passed, available to an **"eligible assessee"** — broadly, any assessee in whose case a **transfer-pricing (TPO) variation** is proposed, and any **foreign company**.

- **What it is:** in eligible cases the AO must first pass a **draft assessment order**. The assessee has **30 days** to either accept it or file **objections** with the DRP. The DRP issues **binding directions** (it must dispose of objections within **nine months** from the end of the month in which the draft order was forwarded), and the AO passes the **final order in conformity** with those directions.
- **Why it matters:** it is a *pre-assessment* dispute-resolution forum that avoids years of appellate litigation for high-value/foreign-company cases and gives the taxpayer a senior-level review before demand is raised.

Module home, menu and roles

After login at the **ITBA Portal Home Page → Assessment Module**, the user reaches the Assessment home page with access to **Screens (Menu)**, **Worklist**, **MIS/Dashboards** and **User Manual/FAQ**. Work is driven by pendencies in the **Worklist**.

Role	Typical actions in the non-faceless flow
AO	Selects cases, generates/signs notices, refers to TPO/VO, makes additions, sends data to CPC-ITR, submits feedback, passes & signs the order
AO Staff	Can prepare/save **drafts** of notices, income computation and order text — but **cannot generate with DSC, cannot send data to CPC-ITR, and cannot pass the order**
Range (Addl./Jt. CIT)	Approves "through approval"/u/s 147 selection, recommends, approves Limited→Complete conversion, grants order approval in search cases
PCIT/CIT	Final approving authority for selection in approval/147/148 categories (PCsIT/CsIT may separately be constituted as a DRP — s.144C)

Features & functions (in brief)

Selection of cases; generation of notice u/s 143(2)/142(1) with/without **DSC**; dispatch register; **e-Proceedings** integration; hearing/adjournment recording; reference to **TPO (s.92CA)** and **VO (s.142A)**; **summons u/s 131**; **notice u/s 133**; **special audit u/s 142(2A)**; **draft order u/s 144C (DRP)**; income computation (additions/disallowances); tax computation via **CPC-ITR**; **Feedback Form**; order generation with **demand notice u/s 156** and penalty notice; **Manual Order Upload**; **Set-aside fresh assessment**; extension of limitation; abatement/revival; and **MIS reports**.

From selection to notice

The remainder of the chapter follows the scrutiny case from selection to order, taking one stage in each subtopic. This first group covers every step up to the point at which a valid scrutiny notice reaches the assessee.

Selection of cases for scrutiny

ITBA supports **five selection categories**: 1. **CASS** (system-based). CASS cases flow **automatically** into the **"Generate Notice to Initiate Proceedings"** screen; no manual selection is needed. 2. **Compulsory Manual** (u/s 143(2), Compulsory category) — AO enters PAN, AY, date of selection and reason (per CBDT's compulsory-selection guidelines); **Submit** creates a notice pendency. 3. **Through Approval** — AO selects, saves and submits; the pendency travels **Range → PCIT/CIT** for approval. Approval taken **offline** can also be captured before submitting for notice generation. 4. **Selection u/s 147 / 153A / 153C** — reassessment / search-linked. For **147** the proposal moves **AO → Range → PCIT/CIT** for sanction, and the notice issued is **u/s 148** (see s.148A below). For **153A**, the AO selects notice years per searched PAN/AY. 5. **Set-aside cases for fresh assessment** (via a dedicated screen — see later).

Limitation for the scrutiny notice — s.143(2)

A scrutiny notice u/s 143(2) must be **served within three months from the end of the financial year in which the return was furnished** (reduced from six months w.e.f. 01.04.2021).

> **Example.** Return for AY 2025-26 furnished on 31.07.2025 (i.e. in FY 2025-26) → notice u/s 143(2) must be served by **30.06.2026**. The system displays the **Limitation Date for Issue** as soon as selection details are entered — a built-in guard against time-barred notices.

The s.148A pre-reassessment procedure (reopening cases)

Before a **s.148** reassessment notice can issue, s.148A (inserted by the Finance Act 2021) requires the AO to: 1. **conduct any inquiry** (with approval of the specified authority) into information suggesting escapement of income; 2. **issue a show-cause notice** giving the assessee **7–30 days** to reply; 3. **consider the reply**; and 4. **pass a reasoned order** on whether it is a fit case to issue a s.148 notice.

The outer time limits (s.149) are **3 years** and **3 months** from the end of the relevant AY, extended to 5 years and **3 months** where the income chargeable to tax which has escaped assessment amounts to or is likely to amount to ₹50 lakh or more (s.149(1), as substituted by the Finance (No. 2) Act, 2024 — Act No. 15 of 2024 — w.e.f. 01.09.2024). *(Reassessment is a distinct chapter of law; the module captures the approval trail and the 148 notice.)*

Notice generation

Path: **Assessment → Menu → Generate Notice to Initiate Proceedings**. The AO picks the section, views the **Selection reason**, enters **date & time of attendance**, can **Preview** the draft, and edits the communication address. - **Without DSC:** email is sent to the assessee and the notice is **shared with e-Filing for e-Proceedings**. - **With DSC:** the notice is signed via **Menu → View/Enter Dispatch Register → Sign Documents** (DSC token attached). For offline service, **Manual Dispatch** records mode/date of service. - **Manual-to-system:** a notice issued offline can be uploaded (issue date, file number, scanned copy) to create the assessment pendency. - A **Limited Scrutiny** flag ("Yes") tells the AO the case is limited in scope; **Limited → Complete Scrutiny** conversion is a separate screen routed to Range/PCIT for approval.

After the notice is generated, an **Assessment Proceeding** pendency appears in the **Worklist**, where it can be delegated to staff with a compliance date.

Cancellation of cases selected

A case selected but **still pending for notice generation** (e.g. selected in error) can be **cancelled** from the **Generate Notice to Initiate Proceedings** screen: select the case, record a **reason of cancellation** (plus approval details for "Through Approval"/148 categories, and supporting documents). On cancellation the case is **deleted from the notice pendency**. An MIS report, *"Cases Cancelled after Selection,"* tracks these.

Conducting the proceeding — hearings, inquiries and references

Once the proceeding is open, the AO gathers material: recording hearings, calling for information, and referring specialised issues out.

Opening the Assessment Proceeding & recording hearings

Opening the workitem from the Worklist, the AO can **Record Hearing** — status **Concluded / Adjourned / Adjourned *sine die*** — with the next hearing date, building the proceeding's history.

Notice u/s 142(1) — questionnaire & calling for information

Via **Initiate Other Actions**, the AO issues a **notice u/s 142(1)** calling for information, accounts and a **questionnaire**. The AO drafts the notice and questionnaire text and generates it (staff can only **save draft**), later signing with DSC via the dispatch screen. Non-compliance with a 142(1) notice is a trigger for **best-judgment assessment u/s 144**. The same **Initiate Other Actions** menu also offers: - **summons u/s 131**; - **notice u/s 133** (power to call for information); - **further notice u/s 143(2)**; - **special audit u/s 142(2A)**; and - **extend limitation**.

Reference to the TPO — s.92CA (in the workflow)

The AO selects the reason and the TPO, captures the approval taken offline, and submits — this **creates a TPO pendency and extends the limitation date**. The TPO's order, once passed, is visible to the AO in **Case History notings**; an offline TPO order can also be uploaded directly.

Reference to the Valuation Officer — s.142A (in the workflow)

The AO enters the VO and asset details, previews/generates the **reference letter**, and later records the **Valuation Report** — which **extends the limitation date**.

Draft order, income computation and tax

With inquiries complete, the AO computes the assessed income and (in eligible cases) routes it through the DRP draft-order path before finalising the arithmetic at CPC-ITR.

Draft order u/s 144C (DRP path)

In **eligible-assessee** (TP-variation / foreign-company) cases, the AO generates a **draft assessment order with DSC**. The assessee's response is captured as **Accepted**, **No response (deemed accepted)**, or **Objection filed**. If objections are filed before the **DRP** (within 30 days), the income is **"frozen,"** and the AO ultimately passes the **final order in conformity with the DRP's binding directions**.

Income computation — additions & disallowances

On the **Income computation** screen the AO selects the **base return/order**; ITBA then displays the ITR-form-specific **schedules** (Salary, BP, CG, OS, CYLA, BFLA, CFL, VIA, SI, etc.) with base figures. The AO enters **additions/disallowances**, and the **Modifications** and **Assessed Income** columns update. If the return is **not filed** or the assessee **ignores the 142(1) notice**, the AO can **convert the case to s.144 (best judgment)**. Departmental *Do's* stress completing all mandatory/interconnected schedules (Bank details, Part A-General, Nature of Business, Sch OI) so the computation is correct.

Sending data to CPC-ITR & tax computation

Only the **AO (not staff)** can **send the data to CPC-ITR** for **tax matching and computation of income, tax and interest**. CPC-ITR returns the computed **Income / Modifications / Tax / Interest** and a **Matching Summary** (challans; TDS/TCS as per 26AS vs as allowed by the AO; extra credit). The AO may **unfreeze** the data to edit and recompute. *(Centralising the arithmetic at CPC-ITR keeps tax/interest computation uniform and error-free across the country.)*

Finalising, passing and serving the order

The concluding stage: mandatory feedback, generation of the signed order, the resulting demand notice, and the limitation that governs completion.

The Feedback Form (mandatory before order)

It is **mandatory to submit the Feedback Form (first tab) before the order is passed**. It captures reasons / quality-case marking and, post-order, feedback on penalty u/s 271(1)(c) (the legacy screen label; for AY 2017-18 onwards the substantive provision is s.270A — see Chapter 09 and prosecution. The order screen will not let the AO proceed without it.

Passing the Assessment Order

Path: **Enter Assessment Order details**. The AO enters the **rich-text order** (which must reflect the **latest** CPC-ITR figures), selects accompanying documents (e.g. **penalty notice**, demand notice), enters the date/time of attendance for the penalty notice, and **generates the order with DSC**. Before generating, the AO should confirm that: - the **Feedback Form** has been submitted; - the computation results have been received and are in **unfreeze** mode; - the "last computation done" and "order generation" fall in the **same month** (otherwise the interest changes); - Range approval has been obtained in search cases; and - no Initiate-Other-Action item is still pending.

The order is passed **u/s 143(3)** (regular) or **s.144** (best judgment). On generation, the module: 1. creates the **demand notice u/s 156** (or the refund); 2. raises a **penalty proceeding** in the Penalty module; and 3. tracks the order under **Menu → List of Demand/Refund Orders**.

Notice of demand — s.156 (what & why)

A **notice of demand u/s 156** is the formal notice served on the assessee stating the **sum payable** (tax, interest, penalty, fine) pursuant to the order. **Why it matters:** it is the legal instrument that makes the demand *recoverable* and starts the **payment clock** (normally 30 days); without a valid 156 notice, there is no enforceable demand.

Limitation for completing the assessment — s.153

The completed assessment is subject to the **limitation u/s 153(1) — 12 months from the end of the AY** (for AY 2022-23 onwards), **extended by 12 months where a TPO reference is made**. VO/special-audit references and court stays also extend limitation (auto-computed by the system). Set-aside fresh assessments run under **s.153(3)/(5)**.

Manual Order Upload

Path: **Assessment → Menu → Manual Order Upload**. Used to bring an order **passed outside the system** onto ITBA. Working through the screen, the AO: 1. enters PAN, category and order type; 2. records **TDS/TCS and challan credit** and the **demand/refund** details; 3. nullifies any earlier demand where required; 4. attaches the order copy; and 5. uploads the order — on upload, the **details are shared with CPC-ITR for accounting**.

Intimation **u/s 245** (adjustment of refund against demand) can also be issued here. Drafts and uploaded orders are managed under **List of Manual Orders** (draft → edit/delete; uploaded → view/status).

Set-aside and remand workflows

When an appellate or revisional authority sends a matter back, ITBA handles it through two distinct paths depending on which order was set aside.

Set-aside cases for fresh assessment (to AO)

Path: **Assessment → Menu → Selection of Set Aside Cases for Fresh Assessment**. When an appellate/revisional authority **(CIT(A) u/s 250, ITAT u/s 254, PCIT u/s 263/264, or a Court) sets aside/restores** an assessment for **de novo** completion, the AO: 1. enters PAN/AY; 2. selects the relevant row; 3. records the **Appellate Order details and the authority**; and 4. clicks **Initiate Proceedings**.

This recreates an assessment pendency for fresh assessment, with limitation running under **s.153(3)/(5)**. An MIS report, *"Set Aside Cases Details,"* tracks them.

Set-aside cases to CIT(A)

Where the **first appellate order itself is set aside** by the ITAT/Court and remanded to **CIT(A)** for fresh disposal, the matter is handled in the **Appeal (CIT-A) module / e-Appeals** rather than in the AO's Assessment worklist. The AO's role is limited to **giving effect** to the eventual appellate order and, if the assessment is restored, to taking up the case again as a **set-aside fresh assessment** (as above). *(The faceless first-appeal scheme operates separately — see the Appeals chapter.)*

Allied functions

- **Extension of Limitation Period** — system auto-extends for TPO/VO/special-audit references; manual extension (court stay etc.) is captured with category and start/end dates.
- **Abatement & Revival** of assessment proceedings (e.g. on search-related abatement) — Menu screens to Abate/Revive a pending proceeding with reason.
- **Assignment of Cases u/s 120(4)/120(5)** to a Range; **Migration of cases from legacy AST/ITD to ITBA**.

Legal & procedural references

- **s.142(1)** — calling for return/accounts/information (notice & questionnaire); **s.142(2A)** — special audit.
- **s.142A** — reference to **Valuation Officer**.
- **s.143(1)** — summary processing / intimation (at CPC-ITR).
- **s.143(2)** — scrutiny notice; **time limit: 3 months from end of FY in which return furnished**.
- **s.143(3)** — regular (scrutiny) assessment order; **s.144** — best-judgment assessment.
- **s.147 / 148 / 148A** — reassessment (income escaping assessment); **s.149 — reassessment time limits (3 years and 3 months / up to 5 years and 5 months where escaped income is ₹50 lakh or more; substituted by the Finance (No. 2) Act, 2024, w.e.f. 01.09.2024)**; **s.153A / 153C** — search assessments.
- **s.92CA** — reference to **Transfer Pricing Officer (TPO)** for arm's length price.
- **s.144C — Dispute Resolution Panel (DRP)** / draft order for eligible assessees (30-day objection; DRP directions binding, 9-month disposal).
- **s.153** — time limits for completion (assessment **12 months** from end of AY for AY 2022-23 onwards; **+12 months** for TPO reference); **s.153(3)/(5)** — set-aside/fresh assessment limitation.
- **s.156** — notice of demand; **s.245** — adjustment of refund against demand; **s.131 / 133** — summons / power to call for information; **s.271(1)(c)** — penalty for concealment; **s.120(4)/120(5)** — jurisdiction/assignment.
- Systems: **CASS, ITBA, CPC-ITR, e-Filing e-Proceedings, DSC**.

Key Takeaways

- **Four assessment types to distinguish: 143(1)** summary/intimation (machine, CPC), **143(3)** scrutiny (detailed, AO), **144** best-judgment (no return/no compliance), **147** reassessment (income escaped, via **148A → 148**).
- **CASS** selects the bulk of scrutiny cases against **objective risk parameters**, giving fairness and removing discretion; it produces **Limited** or **Complete** scrutiny and its cases appear directly in the **Generate Notice** screen. Compulsory-manual selection runs alongside on CBDT criteria.
- **Notice u/s 143(2)** must be served within **3 months from the end of the FY in which the return is furnished** (was 6 months pre-01.04.2021); ITBA shows the **Limitation Date for Issue**.
- **AO Staff can only save drafts**; only the **AO** can **generate with DSC, send data to CPC-ITR, and pass the order**.
- **References to TPO (s.92CA), VO (s.142A) and special audit (s.142(2A)) all extend the limitation date;** the TPO's ALP order is **binding** on the AO.
- **Tax computation is done by CPC-ITR** (matching + income/tax/interest); the **Feedback Form must be submitted before** the order is generated, and the last computation and order generation should fall in the **same month**.
- The order is passed **u/s 143(3)** (or **144**); generation creates the **demand notice u/s 156** and a **penalty proceeding**, and shares data downstream.
- **s.153(1):** complete the assessment within **12 months** from the end of the AY (AY 2022-23 onwards), **+12 months** where a TPO reference is made.

- **Draft order u/s 144C** is required for **eligible assessees** (TP-variation/foreign company); objections go to the **DRP** (30 days), whose directions **bind** the AO; **no response = deemed accepted**.
- **e-Proceedings** carries notices/responses through the e-Filing portal, creating a paperless audit trail (and enabling faceless working).
- A **wrongly selected case** can be **cancelled before notice generation** (with reason/approval); **Manual Order Upload** brings offline orders in (shared with CPC-ITR for accounting); **Set-aside fresh assessment** is initiated from a dedicated menu after capturing appellate-order details.

Key terms & abbreviations

- **ITBA** — Income Tax Business Application
- **CASS** — Computer Assisted Scrutiny Selection
- **CPC-ITR** — Centralized Processing Centre (Income Tax Returns), Bengaluru
- **AO** — Assessing Officer; **PCIT/CIT** — Principal CIT / CIT; **Range** — Addl./Jt. CIT
- **TPO** — Transfer Pricing Officer (s.92CA); **ALP** — Arm’s Length Price
- **VO / DVO** — Valuation Officer / Departmental Valuation Officer (s.142A)
- **DRP** — Dispute Resolution Panel (s.144C)
- **DSC** — Digital Signature Certificate
- **e-Proceedings** — electronic proceedings via the e-Filing portal
- **Demand notice** — Notice of Demand u/s 156
- **CASS Limited / Complete** — scrutiny confined to flagged issue(s) vs the whole return
- **AST / ITD** — legacy Assessment Information System / Income Tax Department application (pre-ITBA)

08. Faceless Assessment in ITBA (Section 144B)

Applicable to: ITO Paper-V, ITI Paper-IV (NOT MS Paper-IV)

Syllabus reference: Assessment Module (Faceless and non-Faceless) — the faceless workflow in ITBA, the AU/VU/TU/RU units and NaFAC, Initiate Verification, Inter-Unit Communication, personal hearing through video conferencing.

Overview

Faceless assessment is the biggest change to the way the Income Tax Department completes scrutiny assessments. It removes the **physical interface** between the taxpayer and the Assessing Officer: the taxpayer never visits an office, never meets the officer, and does not even know which officer or city is handling the case. The work is done by a **team of specialised units** — Assessment, Verification, Technical and Review — coordinated through a single national hub, the **National Faceless Assessment Centre (NaFAC)** at Delhi. Everything happens electronically through the **ITBA Assessment module** on the Department’s side and the taxpayer’s **e-Filing account** on the citizen’s side. The legal basis today is **Section 144B of the Income-tax Act, 1961**. The scheme rests on the role of each specialised unit, the automatic allotment of cases, and an end-to-end electronic workflow for the scrutiny case — including the “Initiate Verification” and “Inter-Unit Communication” functionalities and the personal hearing through video conferencing.

What “faceless” means

“Faceless” means that at no stage does the taxpayer come face-to-face with the officer deciding the case. Three things are deliberately hidden or removed:

- **No physical meeting** — there is no attendance at an office, no adjournment queue, no personal representation across a table. All notices, replies, documents and orders travel electronically.
- **No known officer** — notices and orders are issued in the name of **NaFAC**, not an individual AO. The taxpayer cannot tell who drafted the notice or which unit is examining the case.
- **No fixed geography** — the case is not necessarily worked by the taxpayer’s local Assessing Officer. It can be handled by a unit sitting anywhere in India (this is called **dynamic jurisdiction**).

Compare this with the **traditional (jurisdictional) assessment**, where a taxpayer in, say, Jaipur is assessed by the Jaipur AO, appears before that AO with an authorised representative, and hands over papers physically. Faceless assessment breaks that one-officer-one-taxpayer link.

Why faceless assessment was introduced

Understanding the “why” makes the whole scheme easier to remember. The reform serves **two audiences** with different benefits.

Benefits to the taxpayer

- **Transparency and a clean record.** Every notice, reply and action is captured electronically in the **Case History/Notings** (the digital order-sheet). Nothing happens “off the record”.
- **Elimination of physical interface** removes the cost, travel and time of appearing before an officer, and removes the discomfort of dealing face-to-face.
- **Reduced discretion, corruption and harassment.** Because the taxpayer does not know the officer and the officer does not meet the taxpayer, the scope for undue influence, rent-seeking or arbitrary treatment falls sharply. Anonymity protects both sides.
- **A real opportunity to be heard** through a defined process — mandatory show-cause notice before any adverse variation, and a personal hearing by video conferencing if requested.

Benefits to the Department

- **Efficiency and even workload.** Cases can be spread across the country, so a busy charge’s pendency can be worked by units elsewhere; officers are used more evenly.
- **Team-based quality.** Splitting the work between drafting (AU), enquiry (VU), specialist advice (TU) and review (RU) means no single officer controls the outcome, improving the quality and defensibility of orders.
- **Dynamic jurisdiction** lets the Department deploy capacity flexibly and de-links assessment from the taxpayer’s location.
- **Standardisation and monitoring.** A common SOP, automated allocation, and centralised MIS/dashboards give consistent processes and better oversight than thousands of independent AOs.

The legal journey: from Scheme 2019 to Section 144B

Candidates should be able to trace how the law reached its present form.

E-assessment Scheme, 2019

Notified on 12 September 2019 (S.O. 3264(E)) under the enabling power of **section 143(3A)**. It created the **National e-Assessment Centre (NeAC)** and Regional e-Assessment Centres (ReACs) with assessment/verification/technical/review units.

Faceless Assessment Scheme, 2019 (as amended in 2021)

The 2019 Scheme was renamed and amended by the **Faceless Assessment (1st Amendment) Scheme, 2021** (Notification No. 6/2021, S.O. 741(E), dated 17 February 2021). This amendment (i) required use of the taxpayer's **registered e-mail account**, (ii) brought in the **Dispute Resolution Panel (DRP)** and **eligible assessee** definitions from **section 144C**, (iii) allowed personal hearing by **"video conferencing or video telephony"**, and (iv) rewrote the full assessment procedure (paragraph 5) with the draft-order / review / SCN steps.

Section 144B — the present operative code

The procedure was lifted from a mere "scheme" into the Act itself as **section 144B** (with effect from 1 April 2021), and then **substituted afresh by the Finance Act, 2022** (w.e.f. 1 April 2022) to become the present self-contained code. NeAC was correspondingly renamed the **National Faceless Assessment Centre (NaFAC)**. Some ITBA screens still show the older "NeAC" label for digital signing — treat NeAC and NaFAC as the same body.

So today the **operative law is s.144B**; the earlier "schemes" explain its lineage and are the reason the ReAC/unit architecture exists.

NaFAC — the National Faceless Assessment Centre

What it is

NaFAC (at Delhi) is the **apex hub and single point of contact** for the entire faceless process. It is the only body that talks to the taxpayer. No unit communicates directly with another unit or with the taxpayer — everything is **routed through NaFAC**.

What NaFAC does

- **Serves all notices and orders** on the taxpayer (u/s 143(2), 142(1), 144, the assessment order, demand notice u/s 156, penalty notices).
- **Assigns the case** to an Assessment Unit through the automated allocation system.
- **Digitally signs** every generated document (notice/letter/order). Until signed, ITBA shows the status "Pending with NaFAC for signing".
- **Routes all inter-unit traffic** — AU↔VU, AU↔TU, and the transfer of the draft/review workitem to the RU.
- **Runs the risk-management examination** on the proposal and returns the Review flag.
- **Transfers out** cases that fall outside faceless (to the Jurisdictional AO) after completion or under the exclusion provisions.

Why it matters

NaFAC is what makes anonymity and single-window contact possible. Because notices carry NaFAC's identity and signature, the taxpayer never learns the officer's name; and because all traffic passes through NaFAC, the Department has one auditable channel for the whole proceeding.

The units of NaFAC

In each **Regional Faceless Assessment Centre (ReAC)** the work is done by four kinds of units, coordinated by NaFAC. In ITBA every unit runs through the usual hierarchy — AO, Range Head (Addl./JCIT), PCIT/CIT, CCIT and PCCIT.

Assessment Unit (AU) — what it is and why it matters

The AU is the **engine of the assessment**. It identifies the issues, calls for information, analyses the material, frames the proposal and drafts the order. The working officer is referred to in ITBA as the **FAO (Faceless**

Assessing Officer), with an **AU Range Head (Addl./JCIT)** who approves most actions. It matters because it is the unit that actually decides the additions/disallowances — but, unlike the old single AO, it cannot finalise the case alone: enquiry, specialist advice and review are farmed out to other units, and NaFAC controls service and signing.

Verification Unit (VU) — what it is and why it matters

The VU is the **field-enquiry arm**. On a reference from the AU it conducts enquiry and verification: issuing summons u/s 131(1)(b), calling for information **u/s 133(6)**, examining records, cross-examination of witnesses, and **issuing a commission u/s 131(1)(d)** to an Executing Officer. Under **s.144B(5)** and a CBDT order the VU can carry out **physical verification** of "any other person" or the assessee, regardless of whether a digital footprint exists. It matters because faceless assessment does not dispense with enquiry: the VU supplies the on-ground verification that the AU cannot do itself while staying anonymous.

Technical Unit (TU) — what it is and why it matters

The TU provides **specialist advice** — legal, accounting, forensic, valuation, transfer-pricing, IT/data and other technical inputs — on a reference from the AU. For example, a TP reference is routed by the TU to the **TPO** (the ITBA limitation date changes only *after* the TU forwards the reference to the TPO through the TP-reference tab), and a valuation reference goes to the **Valuation Officer u/s 142A**. **Legal issues already settled by the jurisdictional High Court or Supreme Court need not be referred to the TU**. It matters because it brings expert competence to bear without the AU having to master every specialism.

Review Unit (RU) — what it is and why it matters

The RU provides an **independent quality check** on the proposal/draft order. It examines the facts, the law, the arithmetic and whether all material points have been covered, and either **concurs** or **suggests modifications**. The RU must also verify the **prima facie correctness of the computation** and flag any issue in the Review Report. It matters because a second, independent set of eyes reduces mistakes and makes the final order more defensible in appeal.

The automated allocation system

What it is

NaFAC does **not** hand-pick which unit gets a case. Allocation is done by an **automated allocation system** — an algorithm that randomly assigns cases (and verification/technical references) to a unit in any one ReAC, using technological tools including **artificial intelligence and machine learning**. Re-allocation is possible (e.g., when the RU suggests variation, the case goes to an AU *other than* the one that drafted it).

Why it matters

Random, machine-driven allocation is the mechanism that delivers anonymity and dynamic jurisdiction. Because neither the taxpayer nor the officer can choose or predict the pairing, the scheme removes the discretion and personal contact that fed harassment and corruption in the old system, while balancing workload across the country.

The SOP for AU/VU/TU/RU — the operating rulebook

What it is

Beyond the Act and the scheme, the day-to-day conduct of each unit is governed by a **Standard Operating Procedure (SOP) for AU/VU/TU/RU**. The governing version is the **SOP dated 3rd August 2022**, which **overrides all earlier SOPs** issued by NeAC/NaFAC. The SOP is organised paragraph-wise (Para C on VU verification, Para D.3 on non-response, Para G.3 on centralised communication, Para J on references to VU, Para L.3 on references to TU, etc.).

Why it matters — key procedural rules

- **Only three grounds** let the AU refer a matter to the VU (Para J); mere non-service of a notice is not one of them. Beyond those, the AU may refer verification to the VU **only with the approval of the PCIT of the AU** (Para J.1.2), and that approval is **mandatory** for J.1.2/J.1.3 references.
- **Reference allocation to VU is pin-code mapped:** the AU refers to the **specific VU unit-head** for the concerned pin-code; the unit-head then assigns to a subordinate AC/DC/ITO on the basis of **geographical proximity, equitable workload, and same-address-same-officer** (with PCIT-VU approval and a fortnightly assignment report).
- **Non-responsive / bounced-email cases:** service is valid if the notice is delivered to the taxpayer's **registered e-filing account** with a real-time alert; NaFAC runs **periodic centralised communication through Insight** (Para G.3) and by **speed post** — and the AU must record the speed-post consignment number, address and delivery status in a **separate paragraph of the assessment order**.
- **ILDP cannot be changed once generated;** the AU must ensure additions are reflected in the **Computation of Income** and must **recompute** (unfreezing the dry-run computation) even where no variation is proposed.
- **Time and natural justice:** if a technical glitch shortens the taxpayer's response time, the AU may grant additional time subject to the time-barring date.
- **Section 241A withholding of refund** (Para S.1) became **inoperative from 1 April 2023** on insertion of **s.245(2)** by the Finance Act, 2023; the AU's role under s.245(2) is now governed by CBDT Instruction No. 2/2023.

The faceless workflow in ITBA — selection to the proposal (ILDP)

The Assessment module is reached at **ITBA Portal > Login > Assessment Module > Worklist > Workitem**. The FAO works mainly from the **Initiate Other Actions** screen inside the assessment proceeding. The steps below cover the first half of a typical **s.143(3)** faceless cycle — from selection of the case up to the Income & Loss Determination Proposal.

Step 1 — Selection, pendency and assignment

A case is selected for scrutiny (e.g., through **CASS** risk parameters or Insight information), a pendency is created on ITBA, and NaFAC **assigns** it to an AU through the automated allocation system. NaFAC serves the **notice u/s 143(2)** intimating that the case has been selected for scrutiny and that assessment will be completed under the faceless scheme.

Step 2 — Notice u/s 142(1) (questionnaire)

From *Initiate Other Actions > Generate Notice u/s 142(1)* the FAO selects the section, drafts the questionnaire, saves the draft, and **Submits for Approval** to the Range Head. A **child workitem** opens in the Range's worklist; the Range may edit, add remarks, and **Approve** or **Send Back**. On approval the FAO generates the notice, which goes **Pending with NaFAC for signing**; once **digitally signed by NaFAC** it is served on the taxpayer. The taxpayer responds **only through the e-Filing portal**, and the response flows back into the ITBA workitem.

Step 3 — Enquiry and evidence gathering

Using Initiate Other Actions the FAO can: - **Issue Summon u/s 131(1)(b) — enter addressee PAN**, information sought and compliance date, submit for Range approval, then generate and sign. - **Calling for Information u/s 133(6)** — similar flow, generated as a notice u/s 133(6). - **Issue Letter to Assessee / ITD user / Any Other Person** — with two "no-approval" variants: an **"Issue Reminder"** to the assessee and **"Seeking Information"** from an ITD user can be generated **without Range Head approval**; all other letters need Range approval. Letters to an ITD user (e.g., the JAO) surface as a workitem in the **Faceless Enquiry module**, and the officer's

Response to Letter returns into the main workitem's Case History/Notings. - Raise a **Verification Request to VU** (see "Initiate Verification", below) or a **Technical Assistance request to TU**.

Step 4 — Show Cause Notice (SCN)

Before making any **variation prejudicial** to the taxpayer, the AU must issue an SCN. A **regular SCN** is drafted, submitted for **Addl. (Range) approval**, then generated and NaFAC-signed. A best-judgment **SCN u/s 144** (issued when the taxpayer fails to comply with notices) can be **generated without Range approval**. A s.144 ex-parte assessment needs **two SCNs** — one u/s 144B(1)(ix) [the s.144 SCN] and one u/s 144B(1)(xii)(b) [the variation SCN]. The SCN must also invite the taxpayer to seek a **video-conference hearing** via the button on the e-filing portal.

Step 5 — Income & Loss Determination Proposal (ILDP)

The FAO makes the additions/disallowances (Tax Computation & Matching), records **TP-adjustment** fields where the TP risk parameter is Yes, and prepares the **ILDP** — the proposal that **replaced the old "draft assessment order"** in regular faceless cases. The ILDP is submitted for **Range Head approval**; on approval the FAO **generates** it and clicks **"Send to NaFAC"**, whereupon the Action Required becomes "Sent to NaFAC" and NaFAC runs **Risk Analysis (RMS)**. Note: **once generated, the ILDP cannot be changed**, and the computation must be recomputed to match it.

The faceless workflow in ITBA — review, order and hand-off

Once the ILDP reaches NaFAC, the second half of the cycle runs through risk analysis, review, the final order and the transfer of records out of faceless.

Step 6 — Risk analysis and the Review flag

NaFAC examines the ILDP under the Board's risk-management strategy (an automated examination tool) and returns a **Review flag**: - **Review flag = No** → Action Required becomes "Submit for approval of Assessment Order"; the FAO proceeds straight to order approval. - **Review flag = Yes** → the **workitem is auto-transferred to the Review Unit**, a portal alert goes to the FAO, and Action Required becomes "For Review".

Step 7 — Review by the RU

The RU AO opens the workitem, views the ILDP in Case History/Notings, records a **decision** from the dropdown, and drafts a **Review Report** (which may concur or suggest modifications). The report is **submitted for approval to the Addl. RU**, who approves or sends it back; the RU AO then **generates** the Review Report (NaFAC-signed), which lands back in the AU's Case History/Notings. The RU also checks the **correctness of the computation**.

Step 8 — Handling review modifications

Back with the FAO, if the Review Report contains modifications the FAO sets **"Whether Review Report contains any Modification" = Yes** and chooses **"Accept all Modifications"** or **"Reject any/all Modifications"** (recording reasons for rejection). Only then can the FAO prepare the **Assessment Order Details**. Where required and within the limitation date, the AU may make a fresh reference to the **TU/VU** even at this stage.

Step 9 — Final assessment order

The FAO enters the order text, selects penalty sections, sets the **"Applicability of Draft Order u/s 144C(1)"** flag, and **Submits for Approval** to the Range Head. The Range (who must also confirm agreement with the FAO's decision on any review modification) **Approves** the order. The FAO then **Generates** the order; the **Assessment Order, Computation Sheet and Notice of Demand u/s 156** are shared for **NaFAC digital signature** and, once signed, served on the taxpayer. The final order is passed **u/s 143(3)** (or **u/s 144** in best-judgment cases), with penalty initiation as recorded.

Step 10 — Post-completion transfer of records

After completion NaFAC **transfers all the electronic records** of the case to the **Assessing Officer having jurisdiction** (JAO) for any further action required under the Act (recovery, rectification, giving effect, etc.).

Draft order under section 144C (eligible assessees)

For an **eligible assessee** under **s.144C(15)(b)** — broadly, any person in whose case a **TP adjustment u/s 92CA** is proposed, or a **non-resident (non-domestic company)** — the AU does **not** pass a final order straight away. Instead it issues a **Draft Order u/s 144C(1)**. ITBA permits *Generate Draft Order u/s 144C* only **after the ILDP, Risk Analysis and Review (if flagged) are complete**. The taxpayer may: - **Accept** the variations (capture acceptance date), or - give **No Response** within the s.144C(2) period, or - **object before the DRP** (capture the application no./date; later capture the DRP order/directions date).

The **limitation date on ITBA updates only when the AU captures the response/no-response**, and — where the assessee goes to the DRP — when the **date of receipt of the DRP order** is entered. On DRP directions the AU prepares the order in conformity with s.144C(13) and NaFAC finalises it.

"Initiate Verification" workflow (AU → VU)

When the AU needs field enquiry it raises a **Verification Request to VU**:

1. **AU AO** — from the Assessment Proceeding, click **Verification Request to VU**, enter the **compliance date**, draft the verification letter, **Submit for Approval** to the AU Range Head. (No notice need be attached — the VU itself generates the appropriate notice.)
2. On Range approval and **NaFAC signing**, a **Verification workitem** opens in the **VU** worklist.
3. The **VU AO** can, from the verification workitem: **View Verification Request**, **Issue Summon u/s 131**, **Calling for Information u/s 133(6)**, **Issue Commission u/s 131(1)(d)** (to an Executing Officer, handled in the Faceless Enquiry module), and raise a **Clarification Request to AU**.
    - A **Clarification Request** is approved by the **Addl. VU**, generated and NaFAC-signed; it opens a clarification child-workitem with the **AU AO**, who files a **Clarification Report** (approved by the AU Range) that returns to the VU's Case History.
4. The VU AO drafts the **Verification Report**, submits it for **Addl. VU approval**, and on approval **generates** it. Once **NaFAC-signed**, the Verification Report lands in the **Case History/Notings of the main assessment workitem** with the AU AO.

In practice, notices to a person with no digital footprint can be issued through Insight to a designated NaFAC mailbox; the VU may **edit the mode of reply** in the pre-set Insight notice (so the reply comes to the VU's designation-based email or office address rather than the e-filing portal); and if a physical-verification report will be **delayed beyond 15 days** the VU must send an **interim report** to the AU via internal communication.

Inter-Unit Communication (IUC)

A separate **Inter-Unit Communication** functionality (*Assessment > Menu > Inter Unit Communication*) lets a user communicate with a **peer at the same level in another unit** (AU ↔ VU ↔ TU ↔ RU; AO ↔ AO, Range↔Range, PCIT↔PCIT), **routed through NaFAC**. Key points:

- It is meant for **reminders and general communication**, **not** for statutory references — use the dedicated functionalities (Verification Request, Technical reference) for those.
- IUC communications are **NOT recorded in the Case History/Notings of the main assessment workitem** (unlike Verification/Clarification reports, which are).
- **Workflow:** select the destination unit/user by **PAN + AY**, draft a **Communication Letter** (AO level needs **Range approval**; Range Head and above do **not** need approval), generate and route via NaFAC;

the destination user submits a **Communication Report** back; the initiator may **Continue Communication** or **Close Communication**.

- In typical use, the **TU** may use IUC to send the AU responses **other than the final report** received from the TPO; and where a **Review Report is pending with 7 days or less of limitation left**, urgency messages are sent FAO→FAO, Unit-head→Unit-head and PCIT→PCIT via IUC.

Personal hearing through video conferencing

In reply to an SCN, the taxpayer (or authorised representative) may **request a personal hearing** using the dedicated **button on the e-filing portal**. Under s.144B such a hearing is conducted **exclusively through video conferencing / video telephony** using CBDT-notified facilities — preserving anonymity while giving a genuine opportunity of being heard. **No in-person appearance** before the unit is permitted. In operation:

- The AU must join using the **"Host" link** received in the Case History Notings or by SMS — **not** the "Attendee" link sent to the taxpayer (the host link contains the word "host").
- The AU must ensure **all identifiers are masked/hidden** before starting the VC (to keep the officer anonymous).
- The VC must be formally **concluded in the ITBA functionality** afterwards.
- If the taxpayer fails to request VC through the e-filing button, the AU may issue **another SCN** specifically enabling the VC request, subject to the limitation date.
- **Cross-examination** of a witness (who has a digital footprint) can be conducted **through VC**, with summons to the witness and a copy to the assessee.

Adjournment requests

An **adjournment request** made by the taxpayer through the prescribed e-filing button is visible to the AU through the **"Hearing" button** in the case workitem. Before submitting the ILDP, the AU must ensure any adjournment request has been duly addressed.

Exclusions and transfer out of faceless

Faceless assessment under s.144B does **not** apply to every case. The scheme itself provides for cases to be **transferred out to the Jurisdictional AO (JAO)**, and some categories are handled outside ITBA altogether.

Cases taken out by statute (s.144B(2) & (8))

- **Section 144B(8)** — NaFAC (with Board approval) may transfer a case to the JAO. Used for **GAAR** invocation and the "exceptional categories" (legal heir where the assessee died after the s.143(2) notice; **strike-off companies**; **de-duplication of PAN**; **business restructuring/amalgamation/merger/demerger** affecting the accounts of the year under scrutiny).
- **Section 144B(2)** — cases such as **NRI, Search & Seizure, Survey, or "partly set aside"** matters are taken **out of faceless**.
- **Central charge / search-and-requisition** cases (s.132/132A → s.153A/153C/158BC), **International Taxation** and **Central Circle** cases are outside the scheme.

Cases handled outside ITBA operationally

- **Non-PAN cases**, **no-digital-footprint** cases (handled from the NaFAC backend), and cases where **pendency could not be created on ITBA for technical reasons** are handled separately, with the details escalated by the PCIT/CCIT of the AU to the designated NaFAC e-mail IDs.

Legal & procedural references

- **ITA s.144B** — Faceless Assessment: the operative code (procedure, NaFAC, AU/VU/TU/RU, automated allocation, VC hearing). Key sub-sections: **144B(2)** transfer out (NRI/search/survey), **144B(5)** verification unit/physical verification, **144B(6) the procedure incl. personal hearing by VC**, **144B(8)** transfer to JAO.
- **s.143(2)** — notice of selection for scrutiny; **s.143(3)** — regular assessment order; **s.144** — best-judgment assessment.
- **s.142(1)** — notice/questionnaire; **s.142A** — reference to Valuation Officer; **s.131 / 131(1)(b) / 131(1)(d) — summons / commission**; **s.133(6)** — calling for information.
- **s.144C** — draft order & DRP route for eligible assessees (definitions in **s.144C(15)**); **s.156** — notice of demand; **s.245(2)** — set-off/withholding of refund (replaced s.241A from 1.4.2023).
- **s.132 / 132A / 153A / 153C / 158BC** — search/requisition (excluded from faceless).
- Enabling power **s.143(3A)/(3B)**; the **E-assessment Scheme, 2019** (S.O. 3264(E), 12.09.2019) was renamed the **Faceless Assessment Scheme, 2019** and amended by the **Faceless Assessment (1st Amendment) Scheme, 2021** (Notification No. 6/2021, S.O. 741(E), 17.02.2021), before being subsumed into **s.144B** and **substituted by the Finance Act, 2022** (w.e.f. 1.4.2022).
- **SOP for AU/VU/TU/RU dated 03.08.2022** (governing; overrides earlier SOPs) and the **FAQ on the SOP dated 22.12.2023**; CBDT Instruction No. 2/2023 (role of AU under s.245(2)).

Key Takeaways

- **Section 144B** is the legal basis of faceless assessment; it grew out of the **E-assessment/Faceless Assessment Scheme, 2019**, was amended in **2021**, and was **substituted by the Finance Act, 2022**.
- The four pillars are **transparency, anonymity, team-based assessment and dynamic jurisdiction**, delivered through **automated (AI/ML) random allocation**.
- **NaFAC (Delhi)** is the single point of contact and the **only** body that serves notices/orders and **digitally signs** documents; no unit talks to the taxpayer or to another unit except **through NaFAC**.
- Four units: **AU** (drafts & decides — the AO is the **FAO**), **VU** (enquiry — s.131, 133(6), 131(1)(d), physical verification), **TU** (specialist/legal/TP/valuation advice), **RU** (independent quality review).
- In ITBA the FAO works from **Initiate Other Actions**; most actions need **Range Head approval**, but an **SCN u/s 144** and a **reminder letter / seeking-information-from-ITD-user** can be generated **without** approval.
- The **ILDP** (Income & Loss Determination Proposal) **replaced the old draft assessment order** in regular cases; after ILDP the case goes to **NaFAC for Risk Analysis**, returning a **Review flag**. **Yes → auto-transfer to RU**; **No → straight to order approval**. The **ILDP cannot be edited once generated**, and the computation must be recomputed to match it.
- **Verification Request to VU** = "Initiate Verification"; the VU's **Verification Report** is filed into the **main workitem's Case History**, whereas **Inter-Unit Communication** is peer-to-peer, for reminders only, and is **NOT** part of the main Case History.
- A **prejudicial variation always needs an SCN**; a s.144 ex-parte order needs **two SCNs** (u/s 144B(1)(ix) and (1)(xii)(b)).
- **Personal hearing is only by video conferencing**; the AU joins with the **Host link**, masks all identifiers, and concludes the VC in ITBA.

- **Eligible assessees (s.144C)** get a **Draft Order** and the **DRP** route; the ITBA limitation date moves only when the AU captures the response/no-response (or the DRP order date).
- **Excluded / transferred out:** search & central charge, international taxation, NRI/survey, GAAR, and "exceptional categories" — under **s.144B(2)/(8)**; after completion, records are transferred to the **JAO**.

Key terms & abbreviations

- **NaFAC / NeAC** — National Faceless Assessment Centre (formerly National e-Assessment Centre); the apex hub at Delhi.
- **ReAC** — Regional Faceless (e-)Assessment Centre, where the units sit.
- **AU / VU / TU / RU** — Assessment / Verification / Technical / Review Unit.
- **FAO** — Faceless Assessing Officer (the AU AO in ITBA).
- **ILDP** — Income & Loss Determination Proposal (replaced the "draft assessment order").
- **RMS** — Risk Management Strategy / risk-analysis examination run by NaFAC.
- **SCN** — Show Cause Notice; **DRP** — Dispute Resolution Panel (s.144C objections).
- **VC** — Video Conferencing (mode of personal hearing).
- **IUC** — Inter-Unit Communication (peer-to-peer, not in main Case History).
- **JAO** — Jurisdictional Assessing Officer (receives records after completion / on transfer-out).
- **ITBA** — Income Tax Business Application; **Insight** — the risk/data platform; **CASS** — Computer Assisted Scrutiny Selection.
- **SOP** — Standard Operating Procedure for AU/VU/TU/RU (governing version dated 03.08.2022).
- **Worklist / Workitem** — the ITBA pending-task list and the individual proceeding.
- **Case History/Notings** — the electronic order-sheet of actions on a workitem.

Part IV — Penalty, Rectification/Recovery, Audit & Appeals

09. Penalty Module in ITBA (including Faceless Penalty)

Applicable to: ITO Paper-V, ITI Paper-IV, MS Paper-IV (all three cadres).

Syllabus reference: ITBA Applications Modules — (h) Penalty; Faceless Penalty Scheme, 2021.

Overview

The **Penalty module** of the Income Tax Business Application (ITBA) is the electronic platform on which penalty proceedings under **Chapter XXI of the Income-tax Act, 1961** are initiated, conducted and disposed. Unlike an assessment, a penalty is almost never a standalone action; it is **triggered from a parent (base) proceeding** (assessment, reassessment, TDS default, appeal effect, TPO order or a search/survey by the Investigation wing) in which the Assessing Officer (or other competent authority) records their **"satisfaction"** that a specified default has been committed. This chapter sets out **what a penalty is** and how it differs from tax, interest and prosecution; the core statutory concepts required (under-reporting versus mis-reporting under s.270A, the mandatory pre-decisional hearing, DIN, and the various immunity and waiver routes); each major penalty section handled in ITBA; and the end-to-end module workflow in both the **manual (non-faceless)** and the **Faceless Penalty** modes.

The module manages the full life-cycle of a penalty proceeding: 1. marking a **potential penalty case**; 2. **initiating** the penalty proceeding; 3. issuing the **show-cause notice u/s 274**; 4. capturing submissions through **e-Proceedings**; 5. **calculating** the penalty; 6. passing the **order**; and 7. raising the consequential **demand u/s 156**.

What a "penalty" is — and why it matters

A **penalty** under the Income-tax Act is a **monetary sanction** imposed on a person for a specified **default or contravention** of the Act — for example, under-reporting income, failing to get accounts audited, failing to deduct TDS, or not complying with a notice. It is **quasi-criminal / civil in character**: it punishes non-compliance and deters future defaults, but (unlike prosecution) it does not result in imprisonment.

Why it matters — to the taxpayer: a penalty is a *fresh liability over and above the tax and interest already due*; it can be a large multiple of the tax involved (e.g. 200% of tax for mis-reporting), so understanding when and how it applies protects the assessee. **To the Department:** penalties are the principal instrument for **enforcing voluntary compliance** — they reinforce the return-filing, audit, TDS and information-reporting obligations on which the self-assessment system depends.

How a penalty differs from tax, interest and prosecution

- **Tax** is the primary charge on income — a *liability*, not a punishment. It is computed on total income at the applicable rates.
- **Interest** (e.g. s.234A/B/C, 220) is **compensatory** — it recompenses the exchequer for delayed payment/deferment of tax; it is automatic, mandatory and formula-driven, with **no discretion and no hearing**.
- **Penalty** is **punitive/deterrent**. It generally requires a **default**, a **recorded satisfaction**, a **show-cause notice** and an **opportunity of hearing**, and (for many sections) the authority has **discretion** on quantum between a statutory minimum and maximum.
- **Prosecution** (Chapter XXII, e.g. s.276C, 277) is **criminal** — it can lead to **imprisonment and fine** through a court, on a higher standard of proof (beyond reasonable doubt), and is entirely separate from

penalty. The same default can, in serious cases, attract both penalty *and* prosecution.

> In summary: interest compensates, penalty punishes the default civilly, and prosecution punishes it criminally. ITBA's Penalty module deals only with the **penalty** layer.

The concept of "satisfaction" and the base proceeding

Most penalties can be levied only if, **during the course of** a base proceeding, the competent authority records that it is "satisfied" a default has occurred. This satisfaction (and, for many sections, its recording in the assessment/appeal order and in a separate direction to initiate penalty) is a **jurisdictional pre-condition** — a penalty initiated without valid satisfaction is liable to be struck down. In ITBA this is captured by first marking the case as a **Potential Penalty Case** from within the parent workitem, before any penalty proceeding is formally initiated.

Under-reporting vs mis-reporting of income (Section 270A)

Section 270A, effective **from AY 2017-18**, is the principal penalty for concealment-type defaults; it **replaced the old s.271(1)(c)** ("concealment / furnishing inaccurate particulars"). Its defining feature is a **two-tier, objective structure** built around two distinct concepts.

What "under-reporting" is

A person is treated as having **under-reported** income where, broadly, the assessed income exceeds the income determined in the return (or, where no return is filed, exceeds the basic exemption / processed income), or where reassessment, MAT/AMT recomputation, etc., increases income. It captures a **shortfall in reported income**, whether from a genuine mistake, an unsustainable claim or an omission — **without** necessarily proving deliberate intent. - **Penalty = 50% of the tax payable on the under-reported income.**

What "mis-reporting" is

Mis-reporting is the *aggravated* sub-set of under-reporting, exhaustively defined in **s.270A(9)**: (a) misrepresentation or **suppression of facts**; (b) **failure to record** investments in the books; (c) claim of expenditure **not substantiated by evidence**; (d) recording of any **false entry**; (e) failure to record any receipt in books having a bearing on total income; and (f) failure to report an **international transaction / specified domestic transaction** under transfer pricing. Mis-reporting connotes an **element of deliberate wrongdoing**. - **Penalty = 200% of the tax payable on the under-reported income** that is in consequence of mis-reporting.

Why the distinction matters

The under-reporting/mis-reporting line decides **both the quantum (50% vs 200%)** and **eligibility for immunity**: immunity u/s **270AA is available for under-reporting but NOT for mis-reporting**. Because s.270A is largely **formula-driven and objective**, it reduces the litigation that plagued the old "concealment vs inaccurate particulars" debate — but the burden of establishing that a case falls within the **s.270A(9)** mis-reporting limbs rests on the Department, and the order must clearly specify **which limb** is invoked.

Immunity, waiver and reduction of penalty (270AA / 273A / 273AA)

Chapter XXI provides three distinct relief routes, each operated by a different authority and available on different pre-conditions: statutory **immunity u/s 270AA** (granted by the AO on the assessee's Form 68), discretionary **waiver/reduction u/s 273A** (PCIT/CIT), and settlement-linked **immunity u/s 273AA** (PCIT/CIT). Each is set out below.

Immunity from penalty and prosecution — Section 270AA

Section 270AA lets an assessee obtain **immunity from penalty u/s 270A and from prosecution** (u/s 276C/276CC) on an assessment/reassessment order, provided: 1. the **tax and interest** demanded in the assessment order are **paid within the time** allowed in the notice of demand; and 2. **no appeal** is filed against that assessment order.

The application is made in **Form 68 within one month** from the end of the month in which the assessment order is received. The AO **shall grant** immunity where these conditions are met and the penalty relates to **under-reporting (not mis-reporting)**.

Why it matters: s.270AA offers a **settlement-style route to finality** — by paying the demand and not litigating, the taxpayer secures relief from penalty and prosecution, while the Department realises the demand quickly and reduces the volume of appeals. It is a *distinct* route from the CIT's discretionary waiver u/s 273A and immunity u/s 273AA described below.

Waiver / reduction of penalty — Section 273A

Section 273A empowers the **PCIT / CIT** to **reduce or waive** penalty (and, for co-operative disclosure cases, to grant relief) in the exercise of discretion — for instance where the assessee has, in good faith, made a **full and true disclosure** of income voluntarily and in good faith, co-operated in enquiry, and paid/arranged to pay the tax. **s.273A(4)** additionally allows waiver/reduction on grounds of **genuine hardship** and **co-operation**. In ITBA this is handled by **CIT / CIT(HQ)** through the **Initiate Waiver/Reduction** flow.

Immunity — Section 273AA

Section 273AA allows the **PCIT / CIT** to grant **immunity from penalty** where the person has made an **application for settlement** and that application has abated, subject to conditions (co-operation, true disclosure). ITBA provides for **Grant of Immunity u/s 273AA** by **CIT / CIT(HQ)**, and for **Withdrawal of Immunity u/s 273AA(4)/(5)** by **PCIT / PCIT(HQ)** where the beneficiary fails to comply with the conditions or is found to have concealed material particulars.

> Note the three immunity/relief routes and who operates them: **270AA** (AO grants, on the assessee's Form 68) · **273A** (PCIT/CIT waiver/reduction) · **273AA** (PCIT/CIT immunity linked to settlement).

Mandatory pre-decisional hearing / natural justice — Section 274

What it is

Section 274(1) provides that **no order imposing a penalty shall be made unless the assessee has been given a reasonable opportunity of being heard.** In practice this means a **show-cause notice (SCN) u/s 274** must be issued, clearly stating the section and the default, and giving the assessee time to reply; where the assessee asks, a **personal hearing** must be allowed (in faceless mode, through **video conferencing**).

Why it matters

This is the **audi alteram partem** ("hear the other side") limb of **natural justice**, and it is *not* a formality: - A penalty order passed **without** a valid SCN, or on a notice that **fails to specify the exact charge/limb** (e.g. an omnibus notice that does not strike out the inapplicable ground), is routinely **quashed** by appellate authorities and courts. - Under the faceless framework the requirement is sharpened into a **pre-decisional opportunity**: no order **adverse** to the assessee may be passed without first serving the draft/SCN and allowing a hearing. Omitting it renders the order liable to be set aside irrespective of merits.

For the Department this means the SCN, the reply, the hearing record and the reasoned order must all be captured on the system — which is precisely what the ITBA Penalty module's **Record Hearing / Hearing Order Sheet / Hearing Calendar** screens are for.

Document Identification Number (DIN) on penalty notices

- Every penalty notice and order must carry a computer-generated DIN under CBDT Circular No. 19/2019 dated 14.08.2019 (w.e.f. 01.10.2019); a communication issued without a DIN is invalid and deemed never issued (see Chapter 02 for the full DIN framework). Manual issue is permitted only in narrow exceptional circumstances, with recorded reasons and prior written approval of the CCIT/DGIT, followed by regularisation with a DIN.

Because the Penalty module generates the SCN and order through ITBA, DIN allotment is **automatic** in the normal flow — a key reason penalty proceedings are conducted on the system rather than on paper.

The Penalty Module in ITBA — access and users

Accessing the module

1. Open **https://itba.incometax.gov.in** and **log in** with the **User ID, Password and RSA** token.
2. On the post-login portal home page, click **Penalty** under the **Modules** tab; the **Penalty Home Page** opens.
3. From the Penalty menu, open the **Worklist** (pending workitems) or the **MIS Reports / Dashboards** (monitoring).

Who can levy penalty (users of the module)

Penalty can be levied by a range of authorities depending on the section and the parent proceeding. ITBA provisions roles for: - **AO, Range Head (Addl./JCIT), PCIT/CIT, CCIT/PCCIT** - **DGIT(Inv), PDIT/DIT(Inv), Investigation Unit Head, Investigating Officer, PDIT(I&CI)** (search/survey-linked penalties) - **CIT(A), CIT(DRP), TPO**

All the above, **plus Member and Chairperson, CBDT**, have access to **MIS and Dashboards** for the Penalty module (monitoring/oversight only).

Penalty module workflow (manual / non-faceless) — step by step

Step 1 — Enter / mark Potential Penalty

From the parent workitem (e.g. **Assessment Workitem → Initiate Other Actions → Enter Potential Penalty Details**) the AO records **PAN** (name/address auto-populate), **AY**, the **penalty section**, **remarks** and the **base notice/order**. On submit, the case appears in the **List of Potential Penalty Cases**. This step operationalises the “satisfaction recorded in the base proceeding” requirement.

Step 2 — Initiate Penalty

The user selects the potential case (or navigates directly to **Initiate Penalty**), confirms **section and AY**, **attaches documents** and initiates the proceeding. A penalty workitem is created in the **Penalty Worklist**.

Step 3 — Generate Show-Cause Notice u/s 274

The statutory **SCN** (with **DIN**) giving the assessee an **opportunity of being heard** is generated and served through **e-filing / e-Proceedings**; the assessee views it under **View/Download Notices**.

Step 4 — Record submissions / hearing

Replies are filed online and viewed under **e-Proceedings**. The officer maintains the **Hearing Order Sheet**, uses **Record Hearing**, and schedules through the **Hearing Calendar** — building the natural-justice record.

Step 5 — Calculate Penalty

The officer enters the **amount / number of defaults**; the system computes the **minimum and maximum** leviable penalty for the chosen section, keeping quantum within statutory limits.

Step 6 — Preview & Generate Penalty Order

The **draft order** is previewed and the **final order** passed — or a **dropping order** issued if no penalty is warranted. On levy, **demand u/s 156** (with computation and notice of demand) is generated and posted to **CPC-ITR** for accounting; the signed order/notices flow to **e-filing** for the assessee to view/download.

Allied flows in the module

- **Waiver / Reduction u/s 273A — CIT / CIT(HQ)** selects the penalty order / SCN (e.g. u/s 271(1)(c)) on which relief is sought, and passes a **Waiver / Reduction / Rejection** order via the Worklist.
- **Grant of Immunity u/s 273AA — CIT / CIT(HQ)** selects cases where a penalty SCN has been issued and passes the **immunity order**.
- **Withdrawal of Immunity u/s 273AA(4)/(5) — PCIT / PCIT(HQ)** selects immunity-granted cases and passes a **withdrawal** order under the relevant sub-section.

Principal penalties at a glance

The module handles the following principal penalties; each is summarised below and consolidated in the table that follows.

s.270A — Under-reporting / mis-reporting of income

Discussed in detail above. **50%** of tax on under-reported income; **200%** where the under-reporting is in consequence of **mis-reporting** (s.270A(9)). Levied by **AO / faceless AU**. Replaced the old **s.271(1)(c)** from AY 2017-18.

s.271AAB — Undisclosed income found in a search (s.132)

Applies where a **search u/s 132** was initiated (on or after 15-12-2016) and undisclosed income is found for the "specified previous year". - **30%** of undisclosed income if the assessee **admits** it in the s.132(4) statement, substantiates the manner of derivation, pays tax + interest and declares it in the return; **60%** in **any other case** (not admitted). Levied by the **AO** (Investigation-linked).

s.271AAC — Income taxed u/s 115BBE (unexplained cash credits, etc.)

Where assessed income includes items u/s **68, 69, 69A/B/C, 69D** charged to tax at the special rate u/s **115BBE**. - **Penalty = 10% of the tax payable** u/s 115BBE. Levied by the **AO**. (not attracted where the income was declared in the return and tax paid; and excluded where penalty is leviable u/s 271AAB in search cases).

s.271AAD — False / omitted entries in books of account

Where, in any proceeding, it is found that the books contain a **false entry** or an **entry relevant for computing income has been omitted** to evade tax (targets fake/bogus invoices, e.g. GST-linked bill-trading). - **Penalty = a sum equal to the aggregate amount of such false or omitted entries** (i.e. 100%). A like penalty can be levied on any **other person** who causes the false entry. Levied by the **AO**.

s.271B — Failure to get accounts audited (s.44AB)

Failure to get accounts audited or to furnish the audit report by the due date. - **Penalty = 0.5% of total sales/turnover/gross receipts, subject to a maximum of ₹1,50,000.** Levied by the **AO**. (No penalty if **reasonable cause** shown u/s 273B.)

s.271C — Failure to deduct TDS

Failure to deduct tax at source (or to pay TDS on certain perquisites/dividends as required). - **Penalty = a sum equal to the tax not deducted.** Levied by the **Joint Commissioner (JCIT) — not the AO**.

s.271D / s.271E — Contravention of s.269SS / s.269T (cash loans/deposits)

- **271D:** taking/accepting a **loan, deposit or specified sum ≥ ₹20,000 in cash** (contravention of **s.269SS**).
- **271E: repaying** a loan/deposit/specified advance ≥ **₹20,000 in cash** (contravention of **s.269T**).
- **Penalty in each case = a sum equal to the amount of the loan/deposit/repayment.** Levied by the **JCIT**. (Reasonable-cause defence u/s 273B available.)

s.272A — Failure to comply with notices / statements / answer questions

Covers a spread of procedural defaults — refusal to answer questions, sign statements, comply with notices u/s 142(1)/143(2)/142(2A), failure to furnish statements (e.g. u/s 133/206/206C), etc. - **Penalty = ₹10,000 for each default/failure** (post-2016 for many limbs); for continuing failures to furnish certain statements/returns, **₹100 to ₹500 per day** during which the default continues (as specified). Levied by the **income-tax authority** concerned / **AO**.

s.272B — Failure to comply with PAN provisions

Failure to comply with the **PAN** provisions (s.139A) — not obtaining/quoting PAN, quoting a false PAN, etc. - **Penalty = ₹10,000** (per default, as applicable). Levied by the **AO**.

Section	Default	Quantum (indicative)	Levied by
270A	Under-/mis-reporting of income	50% of tax; **200%** for mis-reporting	AO / faceless AU
271AAB	Undisclosed income found in **search**	**30%** (admitted) / **60%** (otherwise) of undisclosed income	AO
271AAC	Income u/s 68–69D taxed u/s 115BBE	**10%** of tax payable	AO
271AAD	**False / omitted entries** in books	100% of aggregate false/omitted entries	AO
271B	Failure to get accounts **audited** (s.44AB)	0.5% of turnover, **max ₹1,50,000**	AO
271C	Failure to **deduct** TDS	Equal to tax not deducted	**JCIT**
271D / 271E	Contravention of **269SS / 269T**	Equal to loan/deposit/repayment	**JCIT**
272A	Non-compliance with notices / statements	₹10,000 per default; ₹500/day for continuing defaults u/s 272A(2) (w.e.f. 01.04.2022)	AO / IT authority
272B	**PAN** defaults (s.139A)	**₹10,000**	AO

Reasonable cause — Section 273B

For many of the above (271B, 271C, 271D, 271E, 272A, 272B, etc.), **s.273B** provides that **no penalty shall be imposed if the assessee proves reasonable cause** for the failure. This is a key defence the officer must consider before levy — and a common ground on which penalties are dropped or set aside.

The Faceless Penalty workflow

The Faceless Penalty Scheme, 2021 — what it is and why it matters

The **Faceless Penalty Scheme, 2021** was notified vide **CBDT Notification No. 2/2021 — S.O. 117(E) dated 12-01-2021** under **s.274(2A)**, with implementation **directions in Notification No. 3/2021 — S.O. 118(E) dated 12-01-2021** under **s.274(2B)**. It extends the faceless philosophy (already applied to assessment u/s 144B) to

penalty proceedings: - **no physical interface** between the assessee and the department; - **automated allocation** of cases and **team-based** working; - **dynamic jurisdiction** and functional specialisation (drafting unit vs review unit); - decisions taken by **units, not named officers**, to improve consistency and reduce discretion/corruption risk.

Why it matters: it makes penalty proceedings **transparent, geography-agnostic and consistent**, and — crucially — bakes the **pre-decisional hearing** and DIN requirements into a standardised electronic process, so procedural safeguards are less likely to be missed.

From NFPC/RFPC to NaFAC — the structure

The Scheme envisaged a **National Faceless Penalty Centre (NFPC)** and **Regional Faceless Penalty Centres (RFPC)**, with **Penalty Units (PU)** to conduct proceedings and **Penalty Review Units (PRU)** to review draft orders. In practice, per **para 4(4)** of the Scheme read with **CBDT's order dated 20-01-2021**, the **NaFAC / ReFAC act as the NFPC / RFPC** — i.e. the faceless penalty machinery was **subsumed into the National Faceless Assessment Centre (NaFAC/NeAC)** so that faceless penalty runs within the same faceless structure as assessment.

Scope

The faceless mode is used principally for penalties arising out of **faceless assessment (s.144B)** proceedings; certain penalties (e.g. those requiring the JCIT, or search-linked penalties) and cases excluded by CBDT continue in the appropriate channel.

The faceless penalty flow in ITBA (roles and approvals)

1. **AU/VU AO** records **Potential Penalty Details** (PAN, AY, section, remarks, base notice) — *Assessment Workitem → Initiate Other Actions → Enter Potential Penalty Details* — and **submits to the AU/VU Range Head**. Pendency is created in the **List of Potential Penalty Cases**.
2. **AU/VU Range Head** reviews the list, and either proceeds to **Initiate Penalty** (pre-filled screen) or marks **"case not fit"** to reject it.
3. **AU AO** files the **Initiate Penalty** proposal with attachments → pendency goes to the **AU Range Head** worklist.
4. **AU Range Head** views the details/attachments and **Approves** the proposal, or **sends it back to the AU AO** for clarification.
5. After approval, **AU AO** can **generate the hearing/show-cause notice, calculate the penalty, and generate the penalty (or dropping) order** — but **only after AU Range Head approval** at each decisive stage.
6. The draft penalty order is routed to **NeAC/NaFAC for review/signing**; then to **CPC-ITR for accounting**. Once the **order, computation and demand notice** are signed, they are pushed to **e-filing** and appear in the assessee's **View/Download Letters/Notices/Order** screen.

> On approvals: in faceless mode the **Range Head's approval is a mandatory pre-condition** — the AU AO cannot generate the hearing notice or the order without it; NaFAC reviews and signs the order; and CPC-ITR accounts for the demand.

Time limit for passing a penalty order — Section 275

For **FY 2024-25 / AY 2025-26** (Finance (No. 2) Act 2024 and earlier), the **bar of limitation u/s 275** applies (the Finance Act 2025 standardisation is not in force for this exam cycle). Broadly: - Where the relevant **assessment/order is subject to appeal** before CIT(A)/JCIT(A) or revision u/s 263/264 — the penalty may be passed up to the **end of the financial year in which the proceedings are completed, or six months from the**

end of the month in which the appellate/revision order is received, **whichever is later**. - In **other cases** — by the **end of the financial year in which the proceedings are completed**, **or six months from the end of the month in which penalty action is initiated**, **whichever is later**. - For penalties **not connected to assessment** (e.g. some 271C/271D/271E cases) shorter, independent limits apply.

Because a time-barred order is void, the **s.275 clock** is tracked in ITBA as part of the workitem.

Consequences of levy — demand u/s 156

A penalty order creates a **demand**, for which a **notice of demand u/s 156** is generated with the computation and served through e-filing. The demand is posted to **CPC-ITR** for accounting and appears in the assessee's ledger; recovery, if unpaid, follows the normal demand-and-recovery machinery (interest u/s 220, etc.).

Legal & procedural references

- **Income-tax Act, 1961 — Chapter XXI penalties: s.270A** (under-/mis-reporting; s.270A(9) mis-reporting limbs), **s.270AA** (immunity), **s.271AAB**, **s.271AAC**, **s.271AAD**, **s.271B**, **s.271C**, **s.271D**, **s.271E**, **s.272A**, **s.272B**; **s.273A** (waiver/reduction), **s.273AA** (immunity, incl. (4)/(5) withdrawal), **s.273B** (reasonable cause).
- **Procedure: s.274** (procedure / opportunity of hearing; **s.274(2A)/(2B)** faceless enabling provisions), **s.275** (bar of limitation), **s.156** (notice of demand), **s.144B** (faceless assessment — the parent proceeding).
- **Faceless Penalty Scheme, 2021** — Notification **No. 2/2021, S.O. 117(E)** dated 12-01-2021 (u/s 274(2A)); directions **No. 3/2021, S.O. 118(E)** dated 12-01-2021 (u/s 274(2B)); **NaFAC/ReFAC act as NFPC/RFPC** per para 4(4) read with CBDT order dated 20-01-2021.
- **DIN: CBDT Circular No. 19/2019 dated 14-08-2019**, effective 01-10-2019.
- **ITBA:** Penalty module user manual / overview decks; e-Proceedings and CPC-ITR integration.

Key Takeaways

- A **penalty** is a punitive/deterrent monetary sanction for a **default**; it is distinct from **tax** (primary charge), **interest** (compensatory, automatic, no hearing) and **prosecution** (criminal, imprisonment). ITBA's Penalty module handles only the penalty layer.
- Penalty is almost always **triggered from a base proceeding** where **"satisfaction"** is recorded; in ITBA the case first appears as a **Potential Penalty Case** before being **initiated**.
- **s.270A** (from AY 2017-18, replacing s.271(1)(c)) splits defaults into **under-reporting = 50% of tax** and **mis-reporting (s.270A(9)) = 200% of tax**; the distinction also governs **270AA immunity** (available for under-reporting, **not** mis-reporting).
- A **show-cause notice u/s 274 and a real opportunity of being heard are mandatory** (pre-decisional hearing, with **VC on request** in faceless mode); an omnibus/vague notice or a denial of hearing gets the order **quashed**.
- Every penalty notice/order must carry a **computer-generated DIN** (Circular 19/2019, w.e.f. 01-10-2019); a communication without DIN is **invalid and deemed never issued**.
- Quantum quick-facts: **271AAB** 30%/60% (search); **271AAC** 10% of s.115BBE tax; **271AAD** 100% of false/omitted entries; **271B** 0.5% of turnover, **max ₹1,50,000**; **271C/271D/271E** equal to the tax/loan/deposit; **272A/272B** ₹10,000 per default.
- **271C, 271D and 271E are levied by the JCIT**, not the AO; **s.273B** allows dropping many procedural penalties for **reasonable cause**.

- Three relief routes: **270AA** (AO, on Form 68) · **273A** (PCIT/CIT waiver/reduction) · **273AA** (PCIT/CIT immunity, with PCIT withdrawal u/s 273AA(4)/(5)) — all available in the module.
- The **Faceless Penalty Scheme, 2021** (Notification 2/2021 S.O. 117(E), 12-01-2021, u/s 274(2A); directions S.O. 118(E) u/s 274(2B)) removed physical interface with automated allocation and team-based units; its **NFPC/RFPC were subsumed into NaFAC/ReFAC**.
- In faceless mode the **AU Range Head's approval is a mandatory pre-condition** — the AU AO can generate the hearing notice, penalty or dropping order **only after approval**; the order is **reviewed and signed at NeAC/NaFAC** and **accounted for at CPC-ITR**, with the signed order and demand pushed to e-filing.
- Levy raises a **demand u/s 156**; the order must be passed within the s.275 limitation (for FY 2025-26).

Key terms & abbreviations

- **ITBA** — Income Tax Business Application
- **SCN** — Show-Cause Notice (u/s 274)
- **DIN** — Document Identification Number (Circular 19/2019)
- **AO / JCIT** — Assessing Officer / Joint (or Addl.) Commissioner (Range Head)
- **AU / VU** — Assessment Unit / Verification Unit (faceless)
- **NaFAC / NeAC / ReFAC** — National Faceless Assessment Centre (erstwhile National e-Assessment Centre) / Regional centre
- **NFPC / RFPC / PU / PRU** — National / Regional Faceless Penalty Centre, Penalty Unit, Penalty Review Unit (Faceless Penalty Scheme, 2021)
- **CPC-ITR** — Centralized Processing Centre, Income-Tax Returns
- **MIS** — Management Information System (reports/dashboards)
- **VC** — Video Conferencing (personal hearing)
- **s.115BBE** — special (higher) tax rate on unexplained income u/s 68–69D
- **s.269SS / 269T** — restrictions on cash loans/deposits and their repayment

10. Rectification, Order Giving Effect (OGE) and Recovery in ITBA

Applicable to: ITO Paper-V, ITI Paper-IV, MS Paper-IV (all three cadres).

Syllabus reference: ITBA Applications Modules — (c) Rectification, (d) Recovery, (g) Order Giving Effect.

Overview

This chapter covers three closely linked **post-assessment** functions that a field officer performs on the Income Tax Business Application (**ITBA**). All three change a taxpayer's settled tax position after the main assessment is over, and all three end in the same way — a fresh money event (a revised demand or a refund). **Rectification (s. 154)** corrects an obvious mistake in an order already passed. **Order Giving Effect (OGE)** re-works the assessed figures to implement the direction of a higher authority — an appeal, a court, or a revision order. **Recovery (Chapter XVII-D, s. 220–227)** is the machinery for actually collecting the tax that finally stands due. Understanding these three well matters because they are where "the number on paper" becomes "money in the government account" — and where the taxpayer's right to be heard, to appeal, and to seek a stay all come into play. Each is processed through a dedicated ITBA module, with the computation done on the **CPC-ITR** engine, the order **DSC-signed**, carrying a **DIN**, and issuing a **notice of demand u/s 156** (or a refund).

Part A — Rectification (Section 154)

Section 154: "mistake apparent from the record" and what can be rectified

The narrow gateway — what "mistake apparent from the record" means

The whole of s. 154 turns on one phrase — a **"mistake apparent from the record."** This is a deliberately *narrow* gateway. A mistake qualifies only if it is **obvious, patent and self-evident** — visible on a plain reading of the record, needing no investigation, no fresh evidence, and no long chain of reasoning to establish. Classic examples: an arithmetic/totalling error, a wrong tax rate applied, TDS or advance-tax credit clearly appearing on record but not allowed, a figure carried wrongly from one page to another, or a clear misreading of a mandatory provision.

The opposite is a **debatable issue**. If two views are reasonably possible, or if the "error" can be shown only after argument and interpretation, it is **not** a mistake apparent from the record — however wrong the officer or the assessee thinks the original order is. The correct route for a debatable point is appeal or revision, not rectification.

Why it matters — to the taxpayer: it is a quick, cheap, no-appeal remedy to fix a plain slip (say, missing TDS credit) without the cost and delay of filing an appeal. **To the Department:** it lets an officer correct a genuine error on their own record — including under-charged tax — without reopening the assessment, and it keeps the appellate forums free of trivial arithmetic disputes.

What orders can be rectified

An income-tax authority may amend **any order passed by it**. This includes an assessment order, an intimation or deemed intimation u/s 143(1), a penalty order, an order u/s 154 itself (a rectification can itself be rectified), and appellate/revision orders. The scope covers "any matter" that was considered and decided in the order.

Who rectifies, and how rectification is triggered

The authority owns its own order

The core rule is that **the authority that passed the order rectifies it**: - the **AO** rectifies assessment and penalty orders on their record; - **CIT(A) / JCIT(A)** rectify their own appellate orders; - **PCIT / CIT** rectify their own revision orders; - **CPC, Bengaluru** rectifies its own s. 143(1) intimations.

Suo motu vs. on application

Rectification can begin in two ways: - **Suo motu** — the authority notices the mistake itself and moves to correct it; or - **On application** — by the **assessee** (or a **deductor / collector** for TDS/TCS matters). The Commissioner too can set it in motion.

The mandatory hearing before any adverse change (s. 154(3))

This is a key safeguard. An amendment that **enhances an assessment, reduces a refund, or otherwise increases the taxpayer's liability** can be made **only after giving the assessee notice and a reasonable opportunity of being heard**. A rectification that is purely in the taxpayer's favour (e.g., granting missed TDS credit) needs no such hearing. On ITBA this translates into a system-generated show-cause/hearing notice before an adverse s. 154 order can be finalised.

Time-limits and effect on demand or refund

Outer limit — 4 years (s. 154(7))

No rectification can be made after **4 years from the end of the financial year in which the order sought to be rectified was passed**. Note carefully: the clock runs from the FY of the *order being rectified*, **not** from the assessment year and **not** from the original assessment. (Where the rectification is of an order that itself amended an earlier order, the limit runs from the amending order for the matters it dealt with.)

Disposal of an assessee's application — 6 months (s. 154(8))

If the assessee files a rectification application, the authority must **pass an order within 6 months from the end of the month in which the application is received** — either allowing the amendment or refusing it. This protects the taxpayer from applications lying undecided indefinitely.

Effect on demand or refund (s. 154(6))

Rectification is a computation event. Where the amendment **enhances the assessment or reduces a refund**, a **fresh notice of demand u/s 156** is served for the increased sum. Where it **reduces the assessment**, the **excess already paid is refunded**. Interest under s. 220(2) and s. 244A is re-worked on the revised figures.

The ITBA Rectification workflow

1. The taxpayer files a rectification request on the **e-Filing portal** — for CPC-processed returns it is routed to **CPC**; for cases lying on the AO's record it lands in the AO's ITBA **Worklist**. Alternatively the AO initiates **suo motu** in the **Rectification** module.
2. The AO selects the specific order to be rectified, records the mistake apparent from record, and the system **recomputes** income, tax and interest through **CPC-ITR**.
3. For an **adverse** rectification, ITBA issues the **show-cause / hearing notice** required by s. 154(3).
4. The draft **order u/s 154** is approved and **DSC-signed**; ITBA generates it with a **DIN**, posts the revised **computation sheet**, and pushes the **revised s. 156 demand** (or refund) to the CPC / demand database.

Part B — Order Giving Effect (OGE)

OGE: what it is and which orders it gives effect to

Concept — what OGE is and why appellate effect matters

When a higher forum decides an appeal, revision, or court case, its order does not by itself change the entries in the demand register. Somebody has to **translate the direction into revised figures of income, tax, interest and demand** — that translation is the **Order Giving Effect (OGE)**, passed by the AO. If CIT(A) deletes an addition of Rs 10 lakh, the OGE re-computes the tax as if that Rs 10 lakh were never added and refunds/reduces accordingly; if ITAT restores an addition, the OGE brings the demand back.

Why appellate effect matters — to the taxpayer: an appeal "won" is worthless until the OGE actually reduces the demand and releases the refund with interest; delay in OGE means the taxpayer keeps paying interest and loses use of money they are entitled to. **To the Department:** correct and timely OGE prevents both wrong refunds and loss of legitimate revenue, and closes the assessment cycle. Because of this, the law puts **hard time-limits** on giving effect (see s. 153 below).

Which orders OGE gives effect to

- **Appellate orders: CIT(A) / JCIT(A)** under s. 250, the **ITAT** under s. 254, and the **High Court / Supreme Court** under s. 260A / 261.
- **Revision orders: s. 263** (revision by PCIT/CIT that is prejudicial to revenue) and **s. 264** (revision in favour of the assessee).

The AO recomputes the demand or refund in line with the relief allowed, or the addition sustained/enhanced, in that order.

OGE time-limits (s. 153): fresh assessment vs. recomputation

There is a crucial distinction between *re-doing the assessment* and merely *re-calculating the demand* — they carry very different limitation periods.

Nature of effect	Provision	Time-limit
A **fresh assessment / reassessment / recomputation** in consequence of a finding or direction — typically a **set-aside** for a fresh assessment made over again from the start	**s. 153(3)**	**12 months** from the end of the FY in which the order is **received by** the PCCIT/PCIT/CIT (for revision, from the end of the FY in which the order is **passed**)
Effect given **otherwise than by a fresh assessment** — i.e., a **mere recomputation of demand/refund**	**s. 153(5)**	**3 months** from the end of the month in which the order is received (for revision, passed) by PCCIT/PCIT/CIT, **extendable by a further 6 months** by PCIT/CIT on the AO's written request, for reasons beyond the AO's control

Rule of thumb: a full set-aside sending the case back for a fresh assessment = **s. 153(3), 12 months**; anything that is just re-arithmetic on the existing assessment = **s. 153(5), 3 months (+6)**.

The ITBA OGE workflow

1. On receipt of the appellate / court / revision order, the **Appeal** module (or the AO) creates an **OGE work-item** and links the underlying order.
2. In the **OGE / Order Giving Effect** screen the AO enters the findings — relief allowed, additions deleted or sustained, and any fresh directions.
3. The system **recomputes income, tax and interest via CPC-ITR** and produces the **giving-effect order**.
4. The order is approved, **DSC-signed**, generated with a **DIN**, and the revised **s. 156 demand** (or the refund with **s. 244A interest**) is posted to the demand / CPC database.
5. A **full set-aside** instead flows into the **Assessment** module as a fresh assessment, to be completed within the **s. 153(3)** 12-month limit.

Part C — Recovery (Chapter XVII-D, Sections 220–227)

Notice of demand (s. 156), time to pay and interest

What a "notice of demand" (s. 156) is

A **notice of demand u/s 156** is the formal document that tells the taxpayer exactly **how much** is payable, **to whom**, and **by when**, as a result of an order. Every order that creates a liability — assessment, rectification, OGE, penalty, interest — must be accompanied by a s. 156 notice. It is important because it is the **legal trigger for the payment clock** and the foundation for all coercive recovery: without a valid s. 156 notice there is no enforceable "demand" to recover.

Time to pay and interest on default (s. 220(1) & (2))

- **Time to pay (s. 220(1)):** ordinarily **30 days** from service of the s. 156 notice. With the **prior approval of the JCIT / Range Head**, the AO may **shorten** this period where there is reason to believe delay would be detrimental to revenue.
- **Interest on default (s. 220(2)):** if the amount is not paid within the allowed period, **simple interest at 1% for every month or part of a month** runs on the unpaid amount from the end of that period.

"Assessee in default" and its consequences (s. 220–221)

If the taxpayer does not pay the demand within the allowed (or extended) time, they are "deemed to be an assessee in default" in respect of the unpaid amount. This is a legal status, not just a description — it is the switch that turns on the Department's recovery powers. Once a person is an assessee in default: - they become liable to penalty u/s 221 (which the AO may levy up to the **amount of tax in arrears**, after a hearing); and - the full recovery machinery of Chapter XVII-D (TRO, garnishee, attachment, sale, etc.) becomes available against them.

Why it matters — to the taxpayer: default carries mounting interest, penalty exposure, and coercive action against property and bank accounts. **To the Department:** the "in default" status is the legal precondition for issuing a recovery certificate and using the Second Schedule.

Stay of demand, instalments and the 20% guideline

Stay of demand and instalments (s. 220(3) & 220(6))

The status of "in default" is not automatic if the taxpayer has sought relief. The AO may **extend the time** for payment or allow payment in **instalments** (s. 220(3)). Importantly, where the assessee has filed an **appeal before CIT(A)**, s. 220(6) lets the AO, in their discretion, treat the assessee as **not in default** (i.e., grant a **stay**) on the disputed demand while the appeal is pending.

The CBDT "20% stay" guideline

By administrative instruction (CBDT O.M. F.No. 404/72/93-ITCC dated 29.02.2016, as modified on 31.07.2017, which raised the figure from 15% to 20%), the standard condition for granting stay of the *disputed* demand during the first appeal is that the assessee **pays 20% of the disputed demand**; the balance is then generally stayed until CIT(A) decides. The guideline is not a rigid rule: - the AO/PCIT may require **more than 20%** in strong-revenue cases (e.g., issue already settled in revenue's favour by the jurisdictional High Court/Supreme Court, search-based additions, established history of the assessee losing the same issue); and - the PCIT may permit **less than 20%** where there are rulings in the assessee's favour or the assessment is unreasonably "high-pitched."

Courts have repeatedly held that the 20% figure is a **guideline, not a mandatory pre-deposit**, and that the AO retains genuine discretion; the Office Memorandum does not override the Assessing Officer's discretion or the CIT(A)'s powers under s. 251. **Why it matters:** it balances the taxpayer's right not to pay a disputed demand prematurely against the Department's interest in securing revenue while the dispute is decided.

Waiver of interest (s. 220(2A))

The **PCIT / CIT** may **reduce or waive** the s. 220(2) interest where its payment would cause **genuine hardship**, the default was due to circumstances beyond the assessee's control, and the assessee has cooperated in the recovery/assessment.

The Tax Recovery Officer and the Second Schedule

What a Tax Recovery Officer (TRO) does

The **Tax Recovery Officer (TRO)** is the officer charged with **actually recovering** the arrear demand once a person is an assessee in default. The TRO is the enforcement arm of Chapter XVII-D. On receiving a **Tax Recovery Certificate (TRC)** specifying the arrear, the TRO recovers by the modes in the **Second Schedule** and follows the detailed procedure in the **Income-Tax (Certificate Proceedings) Rules** using the **ITCP-series forms**. In practice the TRO: - draws or receives the TRC; - attaches and sells the defaulter's property; - issues garnishee notices u/s 226(3) (defined below); - arrests and detains defaulters where warranted; - appoints a receiver to manage the defaulter's property; - hears and decides objections or claims made by third parties to attached property; and - tracks each certificate through to closure.

The TRO functions much like a civil court executing a decree.

Modes of recovery — the Second Schedule (s. 222)

Where recovery is pursued through the certificate route, the AO/TRO draws up a **Tax Recovery Certificate**, and the TRO recovers by any one or more of the four Second Schedule modes: 1. **Attachment and sale of the defaulter's movable property;** 2. **Attachment and sale of the defaulter's immovable property;** 3. **Arrest and detention of the defaulter in prison;** 4. **Appointing a receiver** to manage the defaulter's property.

Section 223 fixes which TRO has jurisdiction; ss. 224–225 deal with validity of the certificate and stay/amendment of proceedings.

Garnishee and other direct recovery modes

What a "garnishee" (s. 226(3)) is

A **garnishee** order is a notice served **on a third party who holds money for, or owes money to, the assessee** — most commonly the assessee's **bank**, but also any **debtor**, tenant, or customer — requiring that person to pay the money **directly to the Department** instead of to the assessee, up to the amount of the arrear. Section 226(3) allows this **without going through the Second Schedule**: it is a fast, direct way to intercept the defaulter's funds at source. The person served must comply (or state on oath that nothing is due); if that person pays the assessee in disregard of the notice, they become personally liable to the Department to that extent.

Why it matters — to the Department: it is often the quickest, most effective recovery tool, freezing and pulling bank balances directly. **To the taxpayer:** a garnishee/bank-attachment can immobilise operating funds, so it is a strong signal to resolve the arrear or obtain a stay.

Other recovery modes under s. 226 and beyond

- **s. 226(2):** require the **employer / disbursing officer** to deduct arrears from the defaulter's **salary**.
- **s. 226(3):** the **garnishee** notice described above.
- **s. 226(5):** the AO/TRO may **distrain and sell** the defaulter's movable property directly.
- **s. 227:** recovery through the **State Government** as an **arrear of land revenue**.
- **s. 232:** these modes are **not mutually exclusive** — other lawful modes of recovery are not barred.

Void transfers (s. 281) and adjustment of refund (s. 245)

Section 281 — transfers to defraud revenue are void

To stop a defaulter from stripping assets ahead of recovery, **s. 281** makes any **transfer of assets** (by sale, gift, mortgage, etc.) made **during the pendency of proceedings, or after completion but before the demand is paid**, with intent to defraud revenue, **void as against the Department's claim** — subject to protections for a bona fide transferee for value without notice and for transfers made with the AO's prior permission. This lets the Department reach assets that were dishonestly moved out.

Adjustment of refund against demand (s. 245)

Where a refund is due to a taxpayer who also has an **outstanding demand**, s. 245 permits the Department to **set off (adjust) the refund against the demand**. This must be preceded by a **prior intimation** giving the taxpayer an opportunity to respond, and can only be done against a demand that is genuinely payable (not one that is stayed). On the portal, the taxpayer sees and responds to proposed adjustments.

The ITBA Recovery module and portal linkage

- The **Recovery** module hosts the **Demand and Collection Register (D&CR)**, the consolidated **outstanding / arrear demand**, and the **TRO's Worklist**.

- Within it the AO/TRO **draws and issues the TRC**, records **part-payments**, raises **s. 226(3) garnishee notices**, initiates **attachment**, and generates the **ITCP-series notices and orders** — all **DSC-signed** and **DIN-bearing** — tracking each certificate proceeding to closure.
- **CPC / demand-portal linkage:** every demand raised in ITBA flows to the **central demand database**. The taxpayer sees it under **"Outstanding Demand / Response to Outstanding Demand"** on the **e-Filing portal**, where they can agree, disagree with reasons, or note that it is stayed/adjusted (s. 245). Officers monitor arrears through ITBA/CPC dashboards and **CAP (Central Action Plan)** reports.

Legal & procedural references

- **Rectification:** s. 154 — 154(1) power to amend; 154(3) opportunity of hearing before any adverse change; 154(6) revised demand/refund; 154(7) 4-year outer limit; 154(8) 6-month disposal of an assessee's application.
- **OGE / time-limits:** s. 153(3) (fresh assessment to give effect — **12 months**) and s. 153(5) (mere effect / recomputation — **3 months + 6 months**); underlying orders u/s 250 (CIT(A)), 254 (ITAT), 260A/261 (Courts), 263 & 264 (revision).
- **Recovery — Chapter XVII-D:** s. 156 (notice of demand); s. 220 (when tax payable, 220(2) interest, 220(6) stay, 220(2A) waiver); s. 221 (penalty for default); s. 222–225 and the **Second Schedule** (TRC, TRO, attachment, sale, arrest, receiver); s. 226 (226(2) salary, **226(3) garnishee**, 226(5) distraint); s. 227 (State recovery); s. 232 (recovery modes not exclusive); s. 281 (transfers to defraud void); s. 244A (interest on refund).
- **Refund adjustment:** s. 245.
- **Stay guideline:** CBDT O.M. F.No. 404/72/93-ITCC dated 29-02-2016, modified 31-07-2017 (deposit raised to **20%** of disputed demand).

Key Takeaways

- **s. 154 rectifies only a "mistake apparent from the record"** — obvious, non-debatable errors; a debatable point of law is **not** rectifiable and belongs to appeal/revision.
- Rectification **outer limit = 4 years from the end of the FY in which the order rectified was passed**; an assessee's **application must be disposed of within 6 months from the end of the month of receipt** (s. 154(8)).
- Any rectification that **enhances liability or reduces a refund** requires **prior notice and hearing** (s. 154(3)) and ends in a **fresh s. 156 demand**.
- **OGE translates an appellate/court/revision order into revised figures.** A **set-aside for fresh assessment = s. 153(3), 12 months**; a **mere recomputation = s. 153(5), 3 months (+6 months extension)**.
- OGE gives effect to **CIT(A)/JCIT(A) (250), ITAT (254), Courts (260A/261) and revision (263/264)**; the demand/refund is recomputed via **CPC-ITR**.
- A **s. 156 notice** starts the payment clock — normally **30 days**; unpaid demand attracts **s. 220(2) interest @ 1% p.m.** and makes the taxpayer an **"assessee in default"**, exposing them to s. 221 penalty.
- **Stay pending first appeal** is usually granted on paying **20% of the disputed demand** (CBDT O.M.), but this is a **guideline, not a mandatory pre-deposit** — the AO retains discretion.
- The **TRO** enforces recovery via the **Second Schedule**: attachment & sale of movable/immovable property, arrest & detention, and appointment of a receiver, using **ITCP forms** under a **Tax Recovery**

Certificate.

- **s. 226(3) = garnishee** — a direct notice to a **bank/debtor** to pay the assessee's money to the Department, bypassing the Second Schedule; other quick modes include salary deduction (226(2)) and distraint (226(5)).
- **s. 281 voids fraudulent transfers**; **s. 245** allows adjusting a refund against outstanding demand (after prior intimation). All ITBA orders are **DSC-signed, DIN-bearing**, and demands surface to taxpayers as **"Response to Outstanding Demand"** on the e-Filing portal.

Key terms & abbreviations

- **OGE** — Order Giving Effect
- **Mistake apparent from record** — an obvious, self-evident error correctable without argument (basis of s. 154)
- **Assessee in default** — a taxpayer who has not paid a s. 156 demand within the allowed time; unlocks recovery powers
- **TRO** — Tax Recovery Officer; **TRC** — Tax Recovery Certificate
- **Second Schedule** — the code of recovery procedure (attachment, sale, arrest, receiver)
- **ITCP** — Income-Tax (Certificate Proceedings) forms
- **Garnishee (s. 226(3))** — a third party (bank/debtor) directed to pay the assessee's money to the Department
- **D&CR** — Demand and Collection Register
- **CPC-ITR** — Centralised Processing Centre, Income-Tax Returns (recomputation engine)
- **DIN / DSC** — Document Identification Number / Digital Signature Certificate
- **CAP** — Central Action Plan (arrear / recovery monitoring)
- **20% stay guideline** — CBDT administrative norm for stay of disputed demand pending first appeal
- **s. 245** — adjustment of refund against outstanding demand

11. Audit Module in ITBA

Applicable to: ITO Paper-V, ITI Paper-IV, MS Paper-IV (all three cadres).

Syllabus reference: ITBA Applications Modules — (e) Audit.

Overview

Every rupee the Income Tax Department assesses, collects or refunds is exposed to human error — a missed disallowance, a wrong rate, a deduction allowed twice, an excess refund. **Audit** is the mechanism that detects such errors and secures their correction, so that revenue is not lost and the quality of assessments improves. The Department's work is subject to two parallel post-assessment audits: **Internal Audit**, the Department's own quality check conducted under the direct supervision of the **Pr.CCIT** through the **PCIT/CIT (Audit)** hierarchy, and **Revenue Audit**, the external check by the office of the **Comptroller & Auditor General of India (C&AG)**. The **ITBA Audit module** digitises the Internal Audit stream end to end — arranging auditable cases in priority order, requisitioning records, raising **Audit Memos**, routing them for vetting, recording the reply, driving **remedial action** (rectification, reassessment or revision) and finally **settling** the objection, with registers, MIS and dashboards throughout. The current framework for Internal Audit is **CBDT Instruction No. 02/2024 dated 09/09/2024**, which supersedes the earlier Instruction No. 06/2017. Revenue Audit findings are now handled through the C&AG's **CAG-Connect** portal rather than the ITBA "Revenue Audit" module. Separately, the CIT(Audit) also performs an **annual Information Security Audit** of departmental offices. This chapter also distinguishes all of these from the **special audit of an assessee's accounts u/s 142(2A)**, which is a distinct process.

Internal Audit and Revenue Audit — what they are and how they differ

What Internal Audit is and why the Department audits itself

What it is. Internal Audit is the Income Tax Department examining its *own* completed orders — assessments, refunds, rectifications, appeal effects — to find errors and omissions and get them corrected. It is conducted by dedicated audit officers working under the **PCIT/CIT (Audit)** in each Pr.CCIT region, and is entirely internal to the Department: the auditor and the officer whose order is audited are colleagues in the same organisation.

Why it matters — the revenue-safeguard logic. An assessment order, once passed, is subject to time limits for correction (for example, the window for rectification u/s 154, and the defined windows for reassessment u/s 147/148 and revision u/s 263). If a mistake is not caught and corrected inside those windows, the revenue is lost permanently, and the error may instead be pointed out later by the *external* Revenue Audit, which reflects poorly on the Department. Internal Audit therefore exists to:

1. detect and recover leakage of legitimate revenue;
2. improve the quality of assessments by feeding common-error learning back to Assessing Officers; and
3. pre-empt Revenue Audit by catching mistakes before the C&AG does.

In short, it is the Department policing itself so that both revenue and credibility are protected. The governing framework is **CBDT Instruction No. 02/2024**, the Standard Operating Procedure for handling Internal Audit objections, issued in the faceless environment to strengthen accountability and compliance.

Internal Audit vs Revenue (C&AG) Audit — the core distinction

What Revenue Audit is. Revenue Audit is the *external, constitutional* audit of the Department's tax assessments by the **Comptroller & Auditor General of India (C&AG)** — an authority independent of the executive, deriving power from the C&AG's (Duties, Powers and Conditions of Service) Act, 1971. The C&AG deploys field Revenue Audit Parties / Local Audit Parties that inspect assessment records and communicate their findings through a **Local Audit Report (LAR)**. Serious findings escalate to a **Statement of Facts (SOF)** and then a **Draft Para (DP)**, which may finally appear in the C&AG's **Audit Report laid before Parliament**.

Why the distinction matters. Internal Audit is self-regulation the Department controls; Revenue Audit is outside oversight the Department must answer to. A revenue-audit para that reaches Parliament carries far greater consequence than an internal objection. This is precisely why Internal Audit is designed to reach the error first. Audit of the Department's *own accounting and financial* records is done by yet another wing — the internal audit set-up of the Pr. Chief Controller of Accounts (Pr.CCA), CBDT — which is separate from both of the above.

	Internal Audit	Revenue Audit
Conducted by	ITD's own auditors under **PCIT/CIT (Audit)**	**C&AG's** Revenue / Local Audit Parties
Nature	Self-regulation, quality control	External, constitutional oversight
First communication	**Audit Memo** (with UIN)	**Local Audit Report (LAR)**
Escalation	Major/Minor; Call for Explanation	**SOF → Draft Para → Audit Report to Parliament**
Platform	**Internal Audit module of ITBA**	**CAG-Connect portal**
Legal basis	CBDT Instruction No. 02/2024	C&AG (DPC) Act, 1971

The audit set-up — who does what

Under **Instruction No. 02/2024**, the Internal Audit set-up is under the **direct supervision and control of the Pr.CCIT**, and is organised as a **designation-based hierarchy** rather than as fixed audit parties. The earlier structure of the Internal Audit Party (IAP) and Special Audit Party (SAP) is no longer used. Understanding who sits where explains the vetting, approval and settlement routes described later.

Audit authority	Rank	Role
PCIT/CIT (Audit)	Pr.CIT / CIT	Heads Internal Audit in the region; receives and allocates auditable cases; vets high-value Major Audit Memos; settles accepted Major objections
Addl./Jt. CIT (Audit)	Addl. CIT / Jt. CIT	Vets mid-value Major Audit Memos; settles accepted Minor objections; conducts allocated audit
DCIT/ACIT (Audit)	DCIT / ACIT	Conducts allocated audit; issues Audit Memos below the vetting thresholds
ITO (Audit)	ITO	Conducts allocated audit; issues Audit Memos below the vetting thresholds
Any other officer authorised by PCCIT or PCIT/CIT (Audit)	—	Conducts audit within the authorisation given

Two key definitions run through the instruction:

- **Auditee Officer** — the officer who passed the order under audit, or the successor-in-office. **For orders passed in a faceless manner, the Auditee Officer is the Jurisdictional Assessing Officer (JAO).**
- **Auditor** — the Addl. CIT/Jt. CIT (Audit), DCIT/ACIT (Audit), ITO (Audit), or any other officer authorised by the PCCIT or the PCIT/CIT (Audit).

The **Auditee Officer, Range Head and jurisdictional PCIT/CIT** reply to objections and take remedial action. For charges such as International Taxation, Transfer Pricing, Central Charges and the Exemption Wing, Internal Audit lies with the PCIT/CIT (Audit) reporting to the Pr.CCIT in whose territorial jurisdiction the auditee office is located. At the apex, the **ADG (A&I), under the DGIT (L&R)**, monitors the functioning and performance of the Internal Audit set-up and is the coordinating agency for all PCsIT (Audit).

Auditable cases, allocation and targets

Case selection and allocation. The list of auditable cases is forwarded to the **PCIT/CIT (Audit)** on ITBA, arranged in the order of **audit priority**. Where this is technically not feasible, the list is sent to the designation-based mail id of the PCIT/CIT (Audit). The PCIT/CIT (Audit) then allocates the cases, in priority order, among the Addl./Jt. CIT (Audit), DCIT/ACIT (Audit), ITOs (Audit) and any other authorised auditor, ensuring an equitable distribution of workload.

Annual allocation (para 6.2). The PCIT/CIT (Audit) ensures the following annual allocation:

- **Addl./Jt. CIT (Audit) — 140 cases**, including **at least 20 cases** on the registration process of Charitable Trusts/Institutions.
- **DCIT/ACIT (Audit) — 550 cases.**
- Remaining cases are distributed among the other auditors.

Cases pertaining to registration by the **Exemption Wing** are assigned **exclusively to the Addl./Jt. CIT (Audit)**. Transfer Pricing cases are assigned to an auditor **not below the rank of DCIT**. For Central Charges, TDS, International Taxation, Transfer Pricing and any other charge decided by the Board, jurisdiction is assigned by the PCIT/CIT (Audit) with the **prior approval of the Pr.CCIT**.

Target of auditors (para 4). The auditor's target is to **mandatorily complete the audit of all cases allocated during a financial year by the end of that financial year.**

Re-checking targets (para 5). After the audit, the supervisory authorities re-check some of the cases in which no objection was raised:

Re-checking authority	Cases audited by	Target per month	Target per year
PCIT/CIT (Audit)	Addl./Jt. CIT (Audit) and DCIT/ACIT (Audit)	3	**36**
Addl./Jt. CIT (Audit)	ITO (Audit) and any other auditor	10	**120**

If, on re-checking, a supervisory authority finds that an objection ought to have been raised, the case is sent back to the auditor concerned to raise the requisite objection, and the fact is recorded in the monthly report.

Audit Memos — Revenue Effect and Major vs Minor

From "Audit Observation" to the Audit Memo

Under Instruction No. 02/2024, the practice of raising an "**Audit Observation**" is **discontinued**. Errors and omissions are now raised only as an **objection through an Audit Memo**. For each mistake — even if several arise from the same order, for the same assessee and the same assessment year — a **separate Audit Memo is generated on ITBA with a Unique Identification Number (UIN)**. Any significant issue that is *not* an audit objection is communicated by the auditor to the jurisdictional PCIT/CIT through the PCIT/CIT (Audit).

For TDS and Transfer Pricing cases, where ITBA does not generate the UIN automatically, the auditor constructs it manually:

1. the first 10 characters — the **TAN** of the deductor (TDS) or the **PAN** of the assessee (TP);
2. the next four characters — the **assessment year**; and
3. the final two characters — a **sequential number** from 01 to 99.

For example, the first Audit Memo for A.Y. 2022-23 with TAN AAAA12345A takes the UIN AAAA12345A222301 (the assessment year is written as the four digits of A.Y. 20YY-ZZ, i.e., YYZZ — e.g., 2223 for A.Y. 2022-23).

Revenue Effect — the central measure

Revenue Effect (para 7.7) means the tax effect of the issue raised — the difference between the tax on the total income assessed and the tax that would have been chargeable had that income been increased or reduced by the amount in question, **inclusive of surcharge and cess but exclusive of interest**, except where the chargeability of interest is itself the subject of the objection. Where the objection reduces or increases an assessed loss, the Revenue Effect is the **notional tax** on the income covered. In penalty orders, it is the **quantum of penalty** that remained to be levied, or was levied in excess.

Revenue Effect drives everything downstream: whether the objection is Major or Minor, whether the Audit Memo must be vetted before issue, and who ultimately settles it.

Major vs Minor objection (para 7.6)

Classification	Test
Major	Revenue Effect ≥ **₹10 lakh** — **plus** all Exemption-Wing registration objections, regardless of amount
Minor	All other objections (Revenue Effect below ₹10 lakh)

The classification calibrates the level of attention. Major objections are handled by the jurisdictional PCIT/CIT and settled by the PCIT/CIT (Audit); Minor objections are handled at the Range and settled by the Addl./Jt. CIT (Audit). This balances rigour against efficiency.

Vetting thresholds before a Major Audit Memo issues (para 7.5)

Before a Major Audit Memo is issued, it must be vetted according to its Revenue Effect. The vetting is recorded on ITBA (or, for objections not raised through ITBA, through the designation-based e-mail id):

- Revenue Effect **exceeds ₹1 crore** → vetted by the **PCIT/CIT (Audit)**;
- Revenue Effect **₹50 lakh to ₹1 crore** → vetted by the **Addl./Jt. CIT (Audit)**;
- Revenue Effect **below ₹50 lakh** → **issued by the auditor directly** (ITO/ACIT/DCIT (Audit)), with no higher vetting.

Internal Audit workflow in ITBA

Step 1: Allocation of cases

The PCIT/CIT (Audit) receives the priority-ordered list of auditable cases on ITBA and allocates cases to the auditors as described above. Each auditor then sees the allocated cases in the Audit module worklist.

Step 2: Conduct of audit and requisition of records

The audit is conducted on the records available on ITBA. The auditor examines the closed assessment proceedings in view-only mode — including case history and notings, income computation and tax computation — without disturbing the order. Records **not** available on ITBA must be produced manually to the auditor **within seven days** of requisition. Where records are not produced, the PCIT/CIT (Audit) sends a list to the jurisdictional PCIT/CIT, who ensures production; persistent non-production is escalated, with reasons, to the CCIT concerned.

Step 3: Raising the Audit Memo

The auditor raises one or more **Audit Memos**, each generated on ITBA with a **UIN**, entering the Revenue Effect and supporting material. Objections relating to grant or rejection of registration by the Exemption Wing are also raised on the Audit module (in the main body of the Audit Memo) and sent to the **CIT (Exemption)**, with a copy to the PCIT/CIT (Audit).

Step 4: Vetting (for Major objections)

A Major Audit Memo is vetted before issue according to the thresholds in para 7.5:

1. Revenue Effect exceeding ₹1 crore is vetted by the **PCIT/CIT (Audit)**;

2. Revenue Effect between ₹50 lakh and ₹1 crore is vetted by the **Addl./Jt. CIT (Audit)**;
3. Revenue Effect below ₹50 lakh is issued by the **auditor directly**.

The Audit Memo is then issued, creating pendency in the recipient's ITBA worklist.

Step 5: Reply — Accepted or Not Accepted (paras 8.1 and 8.2)

For a **Major** objection, the jurisdictional **PCIT/CIT** examines it. Where necessary, a report may be called from the Auditee Officer through the Audit module within 15 days; the Auditee Officer replies through the Common Functions module within 15 days; and the PCIT/CIT decides acceptability within 15 days of the report (or of the objection, where no report is called). No remedial action is initiated at this stage.

For a **Minor** objection, the **Range Head** performs the same 15-day report-and-decision cycle.

- **Accepted** → the objection proceeds to remedial action (para 9).
- **Not Accepted (Major)** → the PCIT/CIT communicates the reasons to the PCIT/CIT (Audit) within 15 days. If the PCIT/CIT (Audit) agrees, the objection is settled as dropped within 30 days; if not, the reasons for disagreement are conveyed within 30 days, and the PCIT/CIT reconsiders. The decision of the PCIT/CIT is final, and the objection is then closed by the PCIT/CIT (Audit).
- **Not Accepted (Minor)** → the same cycle runs between the Range Head and the Addl./Jt. CIT (Audit); the Range Head's final view is conveyed with the prior approval of the PCIT/CIT, and the objection is closed by the Addl./Jt. CIT (Audit).

Step 6: Remedial action (para 9)

What remedial action is. Remedial action is the actual corrective step that fixes the error the objection identified, carried out in the relevant ITBA module rather than in the Audit module. For an accepted objection it must be **initiated by the Auditee Officer within 30 days** of receipt of the objection.

- **Major objection, action u/s 263** → the PCIT/CIT proceeds under s.263 **within 45 days** of receipt of the objection; otherwise the Auditee Officer is directed to take appropriate action.
- **Minor objection, action u/s 263** → the Range Head refers the matter to the PCIT/CIT within 30 days; the PCIT/CIT decides within 15 days, and where s.263 is not invoked, communicates within 45 days of receipt for the Auditee Officer to act as deemed fit.
- **Action u/s 154** → if the Revenue Effect exceeds **₹2,00,000**, the Auditee Officer must obtain the **prior approval of the Range Head** before initiating rectification.
- **Action u/s 148A(1)** → communicated to the PCIT/CIT (Audit) through the PCIT/CIT (Major), or to the Addl./Jt. CIT (Audit) through the Range Head (Minor).

Where the remedial action **deviates from the audit objection**, an office note recording the reasons must be placed on record. Within 15 days of completing remedial action, the Auditee Officer sends a report (with the order, demand notice, computation sheet and relevant documents) to the PCIT/CIT (Major) or Range Head (Minor), who forwards it to the PCIT/CIT (Audit) or Addl./Jt. CIT (Audit) within 15 days.

Step 7: Settlement and deemed closure (para 10)

- An accepted **Major** objection is **settled by the PCIT/CIT (Audit)** on receipt of the report.
- An accepted **Minor** objection is **settled by the Addl./Jt. CIT (Audit)** on receipt of the report.
- Objections not accepted are closed in the manner described at Step 5.

Deemed closure. Where the PCIT/CIT (Audit) or Addl./Jt. CIT (Audit) does not respond within **60 days** to a communication of non-acceptance received on ITBA, the objection is **deemed closed**, and must be marked as closed on the Audit module **within a further 30 days**.

Limitation override

Where the statutory or administrative time available for any action is shorter than the timeline in the instruction, the action must be taken within that statutory or administrative limit.

Accountability — Calling for Explanation and Ledger Cards

Calling for Explanation (para 15). Where an accepted **Major objection has a Revenue Effect of ₹10 lakh or more**, the jurisdictional PCIT/CIT may call for the explanation of the officer(s) or official(s) concerned. Where the underlying order was passed by an **Assessment Unit** (a faceless order), the explanation of the Assessing Officer and Range Head then posted — and, if required, other officers under s.144B(4) — is called by **requesting the PCCIT, NaFAC through the CCIT concerned**. Explanation may also be sought from officers who delayed or failed to reply to an objection, or to take remedial action, within the prescribed timelines. Where a **Receipt (Revenue) Audit objection of ₹10 lakh or more is accepted** in a case that Internal Audit had earlier audited but not detected, the PCIT/CIT (Audit) may seek an explanation from the auditor concerned.

Ledger Cards (para 16). A record of mistakes committed by a particular officer is maintained through **Ledger Cards**, kept on **ITBA** for erring assessing officers and available to supervisory officers, to enforce accountability and drive reformative steps.

Monitoring. The **ADG (A&I), under the DGIT (L&R)**, monitors the functioning of the Internal Audit set-up and may inspect the set-up of any region with the DGIT (L&R)'s approval. The **CCIT** reviews progress against Central Action Plan targets quarterly. Each year, the PCsIT (Audit) submit a list of notable and recurring errors to the ADG (A&I) by **30 June**, which is compiled and disseminated to field officers and auditors as a quality-feedback loop.

Revenue Audit (ITRA) and the CAG-Connect portal

Revenue Audit — also called **Income Tax Revenue Audit (ITRA)** — is the external audit of the Department's assessments by the C&AG. The **ITBA "Revenue Audit" module is not used by field formations for the C&AG interface**: it is not connected to the C&AG offices. The audit interface now runs on **CAG-Connect**, the C&AG's single-window, web-based platform for two-way (to-and-fro) communication between the **auditee offices (JAO / IT offices)** and the **Revenue Audit (C&AG)**.

How the CAG-Connect workflow operates

1. The C&AG's field parties conduct their inspection and issue their findings as a **Local Audit Report (LAR)** and Inspection Reports.
2. The **JAO / auditee office** accesses **CAG-Connect** to respond to the audit objections in the LAR and Inspection Reports.
3. The office **uploads supporting documents** and the Department's replies on the portal.
4. The status of each objection is **tracked on a dashboard** on CAG-Connect, providing a shared, current view to both sides.

Serious objections escalate in the usual way — **LAR → Statement of Facts (SOF) → Draft Para (DP) → C&AG Audit Report** laid before Parliament — but the correspondence, replies and document exchange between the auditee offices and the C&AG are conducted through CAG-Connect rather than the ITBA module. Where a Revenue Audit objection is accepted, remedial action follows the same statutory routes as Internal Audit (rectification u/s 154, reassessment u/s 147/148, or revision u/s 263), carried out in the relevant ITBA module.

Information Security Audit by CIT(Audit) — a distinct kind of audit

Beyond auditing assessments, the CIT(Audit) also performs an annual Information Security (IS) Audit of departmental offices under CISO Instruction No. 4 (2023) — a physical and procedural audit of compliance with the ITD Information Security Policy, conducted region-wide with prior intimation to the LISO and reported to the LISO with a copy to the CISO (methodology in Chapter 17).

Special audit u/s 142(2A) — how it is different

Do not confuse any of the above with the **special audit u/s 142(2A)**. Here, during a *pending assessment*, the **Assessing Officer** — having regard to the nature and complexity of the accounts, the volume of accounts, doubts about their correctness, the multiplicity of transactions or the specialised nature of the business, and in the interests of revenue, and with the prior approval of the **PCCIT/CCIT/PCIT/CIT** — directs the **assessee** to get *its own* accounts audited by a **Chartered Accountant nominated** by the PCCIT/CCIT/PCIT/CIT, and to furnish the report in the prescribed form (**Form 6B**). Key differences:

- It audits the **taxpayer's books**, not the Department's order.
- It is done by an **external Chartered Accountant**, not by the CIT(Audit)'s auditors or the C&AG.
- It occurs **during assessment** (an input to the order), not after it.
- It is part of the **assessment workflow**, not the ITBA Audit module.

Four distinct types of audit should be distinguished: **Internal Audit** (the Department audits its own orders), **Revenue Audit** (the C&AG audits the orders), **Information Security Audit** (the CIT(Audit) audits offices' security), and **Special Audit u/s 142(2A)** (a chartered accountant audits the *assessee's* accounts).

Legal & procedural references

- **CBDT Instruction No. 02/2024, dated 09/09/2024 (F.No.240/08/2024-A&PAC-I)** — the current Standard Operating Procedure for handling Internal Audit objections. It **supersedes Instruction No. 06/2017**. Key features: designation-based audit hierarchy under the Pr.CCIT; definitions of "Auditee Officer" (the JAO for faceless orders) and "Auditor"; discontinuance of the "Audit Observation"; objections raised only through Audit Memos with a UIN on ITBA; Major/Minor classification (≥ ₹10 lakh, plus all Exemption-Wing registration objections); vetting thresholds (> ₹1 cr by PCIT/CIT (Audit); ₹50 lakh–₹1 cr by Addl./Jt. CIT (Audit); below ₹50 lakh by the auditor); settlement of accepted objections (Major by PCIT/CIT (Audit), Minor by Addl./Jt. CIT (Audit)); allocation targets (Addl./Jt. CIT — 140 cases incl. ≥20 trust-registration cases; DCIT/ACIT — 550 cases); the 15-day report/decision cycle, 30-day initiation of remedial action, s.263 timelines (45 days Major / 15 days Minor), and 60-day (+30-day) deemed closure; accountability through Calling for Explanation and Ledger Cards; and monitoring by the ADG (A&I) under the DGIT (L&R).
- **CAG-Connect portal** — the C&AG's single-window, web-based platform for two-way communication between auditee offices (JAO/IT offices) and Revenue Audit; used by JAOs to respond to LARs and Inspection Reports, upload documents and track status. The ITBA "Revenue Audit" module is not connected to C&AG offices.
- **CISO Instruction No. 4 (2023)** — methodology, roles and action plan for the annual Information Security Audit by the CIT(Audit); LISO/BISO/CISO roles and checklists (Annexures 1–4).
- **Income-tax Act, 1961** — **s.154** (rectification), **s.147/148** (reassessment of escaped income), **s.148A(1)**, **s.263** (revision by PCIT/CIT), **s.143(3)** (regular assessment), **s.144B** (faceless assessment), **s.142(2A)** (special audit of the assessee's accounts — distinguished; report in Form 6B).
- **C&AG (Duties, Powers and Conditions of Service) Act, 1971** — basis of C&AG Revenue Audit; outputs **LAR → Statement of Facts → Draft Para → C&AG Audit Report** to Parliament.
- **ITD Information Security Policy** and the **ITBA Audit module** user manual.

Key Takeaways

- **Internal Audit = the Department auditing its own completed orders**, under the direct supervision of the **Pr.CCIT** through the **PCIT/CIT (Audit)** hierarchy, to recover revenue and improve quality;

Revenue Audit = the external C&AG audit — arriving as a **LAR** and escalating via **Statement of Facts → Draft Para → Report to Parliament**.

- The current framework is **CBDT Instruction No. 02/2024**, which **supersedes Instruction No. 06/2017**. Internal Audit is a **designation-based hierarchy — PCIT/CIT (Audit) → Addl./Jt. CIT (Audit) → DCIT/ACIT (Audit) → ITO (Audit)** (or authorised officer). The old **IAP/SAP** party structure is discontinued.
- The **"Auditee Officer"** is the officer who passed the order (or successor); **for faceless orders it is the JAO**. The **"Audit Observation" is discontinued** — objections are raised only through an **Audit Memo** with a **UIN** on ITBA.
- **Major objection = Revenue Effect ≥ ₹10 lakh** (plus **all** Exemption-Wing registration objections); **Minor = below ₹10 lakh**. **Revenue Effect** = tax including surcharge and cess, excluding interest (unless interest is itself the objection).
- **Vetting before a Major Audit Memo issues**: **> ₹1 cr → PCIT/CIT (Audit)**; **₹50 lakh–₹1 cr → Addl./Jt. CIT (Audit)**; **below ₹50 lakh → issued by the auditor directly**.
- **Settlement**: accepted **Major → PCIT/CIT (Audit)**; accepted **Minor → Addl./Jt. CIT (Audit)**. **Deemed closure** if Audit does not respond to a non-acceptance within **60 days** (mark closed within a further 30 days).
- **Targets**: audit of all allocated cases completed within the FY; annual allocation — **Addl./Jt. CIT (Audit) = 140 cases** (incl. ≥20 trust-registration cases), **DCIT/ACIT (Audit) = 550 cases**; re-check targets — PCIT/CIT (Audit) 36/yr, Addl./Jt. CIT (Audit) 120/yr.
- **Timelines**: 15-day report/decision cycle; remedial action initiated within **30 days**; s.263 route — PCIT/CIT within **45 days** (Major) / **15 days** (Minor); prior Range-Head approval for a s.154 remedy where Revenue Effect exceeds **₹2,00,000**.
- **Accountability**: explanation may be called for accepted Major objections with Revenue Effect **≥ ₹10 lakh** (for faceless orders, via the PCCIT, NaFAC through the CCIT); **Ledger Cards** of erring officers on ITBA; monitoring by the **ADG (A&I) under the DGIT (L&R)**.
- **Revenue Audit uses CAG-Connect**, not the ITBA Revenue Audit module: JAOs respond to LARs and Inspection Reports, upload documents and track status on a dashboard.
- **Information Security Audit** is a **distinct annual audit by the CIT(Audit)** (CISO Instruction 4/2023): intimate the LISO, plan region-wide, inspect against checklists (Asset/HR/Physical/Incident), report to LISO with a copy to CISO, LISO fixes non-compliances in 15 days.
- Keep four audits apart: **Internal Audit ≠ Revenue Audit ≠ Information Security Audit ≠ Special Audit u/s 142(2A)** — the last is an external CA auditing the **assessee's** accounts during assessment (Form 6B), not part of the ITBA Audit module.

Key terms & abbreviations

- **PCIT/CIT (Audit)** — heads Internal Audit and performs the IS Audit in a region; vets high-value Major Audit Memos; settles Major objections.
- **Auditee Officer** — the officer who passed the order (or successor); the **JAO** for faceless orders.
- **Auditor** — Addl./Jt. CIT (Audit), DCIT/ACIT (Audit), ITO (Audit) or an officer authorised by the PCCIT or PCIT/CIT (Audit).
- **Audit Memo / UIN** — the document raising an internal audit objection and its Unique Identification Number on ITBA.

- **Revenue Effect** — tax impact of an objection (surcharge and cess included, interest excluded unless interest is the objection); decides Major/Minor and the vetting route.
- **Major / Minor objection** — Revenue Effect ≥ ₹10 lakh (Major; plus all Exemption-Wing registration objections) versus below ₹10 lakh (Minor).
- **Deemed closure** — automatic closure of a non-accepted objection where Audit fails to respond within 60 days.
- **C&AG / ITRA** — Comptroller & Auditor General of India / Income Tax Revenue Audit.
- **CAG-Connect** — the C&AG's single-window portal for two-way communication between auditee offices (JAO) and Revenue Audit.
- **LAR** — Local Audit Report (C&AG's communication of a revenue-audit objection).
- **SOF / DP** — Statement of Facts / Draft Para (escalation stages of a Revenue Audit objection).
- **Remedial Action** — corrective step (s.154 / s.147-148 / s.263) taken in the relevant ITBA module.
- **Settlement** — final closure of an audit objection after remedial action.
- **Ledger Card** — ITBA record of mistakes committed by an officer, for accountability.
- **ADG (A&I) / DGIT (L&R)** — the coordinating and monitoring authorities for the Internal Audit set-up.
- **CISO / LISO / BISO** — Chief / Local (region) / Building Information Security Officer.
- **s.142(2A)** — special audit of the assessee's accounts by a nominated CA (report in Form 6B).

12. Faceless Appeal, Appeal Register & CSR, and e-Nivaran

Applicable to: ITO Paper-V, ITI Paper-IV, MS Paper-IV (all three cadres).

Syllabus reference: ITBA Applications Modules — (f) Faceless Appeal, Appeal Register and CSR; (i) e-Nivaran.

Overview

This chapter deals with two connected areas of the department's work, both of which operate within ITBA. The first is the **appellate machinery** — how a taxpayer who disagrees with an order can challenge it, the statutory ladder of appeals (first appeal to CIT(A)/JCIT(A), then ITAT, High Court and Supreme Court), the **Faceless Appeal Scheme, 2021** run through the National Faceless Appeal Centre (NFAC), and the **ITBA Appeal Register & CSR module** through which the department records incoming appellate orders, monitors limitation, and decides whether to file its *own* (departmental) appeals. In this module **CSR means Central Scrutiny Report** — a report that scrutinises an appellate or judicial order and recommends whether to appeal further. The second area is **e-Nivaran**, the department's single-window grievance-redressal system. Beyond the module names and time-limits, it is important to understand *why* a right of appeal and a grievance channel exist at all: they are the two means by which a citizen can be heard when the Department makes an error, and both are central to taxpayer trust and to the **Sevottam** service philosophy.

The right of appeal and the appellate hierarchy

What the "right of appeal" is — and why it matters

An **appeal** is a taxpayer's statutory right to have a higher authority re-examine an order passed against them. When an Assessing Officer (AO) raises a demand, disallows a claim, or levies a penalty, the taxpayer is not left with "the AO's word is final". The Income-tax Act, 1961 deliberately builds in an independent review ladder.

- **Why it matters to the taxpayer:** it is the primary safeguard against a wrong, arbitrary or excessive assessment. It gives a fair, reasoned second look before money actually has to be paid, and it upholds the principle of *natural justice* (the right to be heard).
- **Why it matters to the Department:** appeals discipline assessment quality — orders that will not survive scrutiny get corrected — and they build **public trust and legitimacy** in the tax system. A tax administration that lets its own mistakes be challenged and fixed is more readily accepted. Appellate decisions also settle points of law that guide future assessments.

Importantly, an appeal is **not** available against every action; only against the specific classes of order that the Act makes appealable.

The appeal ladder (statutory hierarchy)

Stage	Forum	Who can appeal	Governing section(s)
First appeal	**CIT(Appeals)** or **JCIT(Appeals)**	Assessee (aggrieved taxpayer)	s.246A (appealable orders), s.249 (form/fee/time), s.250 (procedure), s.251 (powers)
Second appeal	**Income Tax Appellate Tribunal (ITAT)**	Assessee **or** the Department	s.253
Appeal on a substantial question of law	**High Court**	Assessee or Department	s.260A
Final appeal	**Supreme Court**	Assessee or Department	s.261 (appeal) / SLP under Art.136 of the Constitution

Two points are worth noting: - **The hierarchy rises from fact to law.** The first two stages (CIT(A)/JCIT(A) and ITAT) can re-examine **facts and law**. The ITAT is the **final fact-finding authority**. Above it, the High Court and Supreme Court intervene only on a **substantial question of law**, not on findings of fact. - **Both parties may appeal at the higher stages.** The first appeal is a taxpayer's right only, but from the ITAT stage upward the **Department too may appeal** if it loses — which is where the Appeal Register & CSR module comes in.

First appeal — CIT(A) / JCIT(A)

What the first appellate authority is

The **Commissioner (Appeals)** — and, since 2023, the **Joint Commissioner (Appeals)** — is an income-tax authority who sits in judgment over the AO's order. Though part of the Department, the appellate authority acts *quasi-judicially* and independently of the assessment side.

s.246A — appealable orders

Section 246A lists the orders a taxpayer can bring in first appeal — e.g. assessment orders u/s **143(3)**, best-judgment assessments u/s **144**, reassessments u/s **147**, rectification orders u/s **154**, intimations/orders raising demand, TDS orders u/s **200A/201**, and **penalty** orders. If an order is not in this list, no first appeal lies against it (the remedy may lie elsewhere, e.g. revision u/s 264).

s.249 — form, fee and limitation

First appeal is filed in **Form 35**, electronically, within **30 days** of service of the notice of demand or the order appealed against. A modest filing fee applies (graded by assessed income). As a rule, the appeal is entertained only if the admitted tax on returned income has been paid; delay can be condoned for sufficient cause.

s.250 — procedure

Section 250 governs the hearing: fixing a date, hearing the appellant and the AO, calling for records or a remand report, and — crucially — the power to **enhance** an assessment only after giving the appellant a reasonable opportunity to show cause.

s.251 — powers of the first appellate authority

The CIT(A)/JCIT(A) has wide powers: in an assessment appeal to **confirm, reduce, enhance or annul** the assessment; in a penalty appeal to **confirm, cancel, or vary** the penalty. The breadth of these powers is what makes the first appeal a genuine, substantive review rather than a mere formality.

JCIT(Appeals) and the e-Appeals Scheme, 2023

What it is and why it was created

The **Finance Act, 2023** introduced a new first-appellate authority, the **Joint Commissioner (Appeals)** / Addl. CIT(A), to clear the very large backlog of **small-demand** appeals pending before CIT(A). Low-value disputes could now be routed to a dedicated authority, freeing CIT(A) capacity for larger and more complex matters. - **Operationalised through the e-Appeals Scheme, 2023.** Cases can be **transferred** between CIT(A) and JCIT(A) as directed. The JCIT(A) generally handles appeals against orders where the demand/threshold is small. - **Why it matters:** faster disposal of routine, low-stakes disputes — better service for small taxpayers and reduced pendency for the Department.

Faceless Appeal Scheme, 2021 and the NFAC

What the Faceless Appeal Scheme is — and why

The **Faceless Appeal Scheme** makes the disposal of **first appeals by CIT(A)** anonymous, team-based and fully electronic. There is **no physical interface** between the appellant and the appellate authority: the taxpayer does not know (and cannot approach) the particular officer deciding the case, and vice versa.

- **What it is:** a scheme, first notified in 2020 and **replaced by the Faceless Appeal Scheme, 2021** (CBDT Notification No. 139/2021 dated **28.12.2021**, effective from the setting up of NFAC by Office Order dated 29.12.2021), under which appeals are allocated by an automated system to appeal units across the country and decided online.
- **Why it exists / why it matters:**
- *For the taxpayer* — it removes the scope for personal influence, harassment or corruption at the appellate stage, provides territorial neutrality (an appeal from one city may be decided by an officer elsewhere), and gives a documented, digitally-signed order.
- *For the Department* — it improves consistency and efficiency, spreads workload nationally, creates a fully auditable electronic record, and reinforces the wider **faceless** reform (faceless assessment + faceless appeal + faceless penalty) that is the backbone of the modern, technology-driven Income Tax Department.

NFAC — the National Faceless Appeal Centre

What it is: the NFAC (headquartered in Delhi) is the **single point of contact** for the whole faceless appeal process. Every notice, communication and order passes **through** NFAC; the appellant deals only with NFAC and never directly with the deciding officer.

Key change from 2020 to 2021: the 2021 scheme **abolished the Regional Faceless Appeal Centres (RFACs)** that existed under the 2020 scheme. Allocation is now **direct from NFAC to an appeal unit** through an **automated allocation system**, simplifying the structure.

Appeal Unit — who actually decides

What it is: an **Appeal Unit (AU)** consists of one **Commissioner (Appeals)** with supporting income-tax authorities and staff. The AU is the body that actually examines the grounds, calls for records/remand reports (routed through NFAC to the AO/NaFAC), frames the appellate order, and returns it — **digitally signed** — to NFAC for communication.

The faceless appeal workflow

Step by step

1. **Appellant files** Form 35 electronically (the appeal reaches NFAC).
2. **NFAC allocates** the appeal, by automated allocation, to an **appeal unit**.
3. The **appeal unit** issues notices, seeks information, and may call for a **remand report** from the AO — **all routed through NFAC** (no direct contact).
4. The AU **drafts the order**, applies its **digital signature**, and sends it to NFAC.
5. **NFAC communicates the order** to the appellant and to the AO, who then gives **appeal effect** (recomputes demand/refund).

Personal hearing — a right, on request

A major taxpayer-friendly feature of the **2021** scheme: the appellant has a **right to request a personal hearing through video conferencing (VC)**, and on such request the CIT(A) of the appeal unit **shall** allow it. (Under the earlier 2020 scheme this was discretionary; the 2021 scheme made it a matter of right.) All communications remain **exclusively electronic and digitally authenticated**.

Appeal Register & CSR — monitoring departmental appeals in ITBA

What the Appeal Register is — and why it matters

What it is: the **Appeal Register** (also called the **Appeal Receipt Register**) is the ITBA facility in which the Department **records the receipt of every appellate or judicial order** it receives — from CIT(A), ITAT, High Court and Supreme Court. It captures appellate-authority details, date of receipt, subject-matter, and current status, and tracks appeals as **filed, pending or disposed**.

Why it matters: - It **fixes the limitation clock.** The date an order is *received* starts the countdown for filing a further departmental appeal (e.g. 60 days to ITAT). Recording it accurately is what prevents the Department from missing a deadline and losing the right to appeal. - It gives **supervisory visibility** — PCITs/CCITs can see pendency, ageing and disposal at a glance, and it **triggers the CSR workflow** for deciding whether to contest an order.

Access / path: https://itba.incometax.gov.in → **ITBA Portal** → **Login** → **Modules** → **Appeal Register & CSR**.

What the CSR (Central Scrutiny Report) is — and why it matters

What it is: in the ITBA appeal context, **CSR = Central Scrutiny Report** (note: *Report*, **not** "Register"). A CSR is the **structured proforma** in which an appellate or judicial order that has gone *against* the Department is **scrutinised issue-by-issue** to record a reasoned recommendation on **whether to file a further appeal** — and, if so, on what grounds/questions of law.

Why it matters: - It ensures the decision to litigate further is **deliberate and reasoned**, not automatic. Each adverse issue is examined on merits and against monetary limits. - It creates an **audit trail** of who recommended what and who authorised the appeal, and it feeds the **grounds of appeal** / **substantial questions of law** used in the higher forum. - It is the department's core tool of **litigation management** — helping avoid frivolous appeals while protecting revenue in genuine cases.

CSR workflow, roles and departmental second appeals

CSR workflow and roles

Role	Function in the CSR / departmental-appeal flow
AO	Records receipt of the order; analyses it; initiates/prepares the CSR; on a decision to appeal, files **Form 36** (ITAT) and gives appeal effect
Range Head (Addl./JCIT)	Reviews the issues; may draft the **grounds of appeal**; recommends filing or acceptance
PCIT	Records the **final decision** to accept the order or contest it; issues **directions / authorisation** to appeal
CIT (Judicial)	For ITAT/HC matters — reviews the recommendation, drafts/vets the **Substantial Questions of Law**, submits observations
CCIT	Takes the final decision on contesting **High Court** matters; the proforma is forwarded to the **Directorate of Legal & Research (L&R)** where filing is proposed

Indicative routing of departmental appeals:

Against a **CIT(A) order** (first appeal to the ITAT under s.253): 1. the AO records receipt and prepares the CSR; 2. the Range Head reviews the issues; 3. the PCIT authorises the appeal; and 4. the **s.253** appeal is filed with the ITAT.

Against an **ITAT order** (appeal to the High Court under s.260A): 1. the AO prepares the CSR; 2. the Range Head reviews the issues; 3. the PCIT records its recommendation; 4. the **CIT(Judicial)** vets the substantial questions of law; 5. the CCIT takes the final decision; and 6. the **s.260A** appeal is filed with the High Court.

Against a **High Court order** (appeal to the Supreme Court under s.261 / SLP): 1. the PCIT/CCIT record the recommendation; 2. the proforma is forwarded to the **Directorate of L&R**; and 3. the **s.261** appeal / SLP is filed with the Supreme Court.

Appeal effect and the departmental second appeal

- **Appeal effect:** after a CIT(A)/ITAT order, the **AO must give appeal effect** — recompute the demand or refund in line with the order, within the prescribed time. The module tracks pendency of appeal effect so that relief/recovery is not delayed.
- **Departmental second appeal (s.253):** where the Department decides to contest, the PCIT-authorised AO files an appeal to **ITAT** in **Form 36** within **60 days** of receipt of the order — but only **after** CSR scrutiny.

Departmental-appeal monetary limits (Circular 9/2024)

What they are and why they exist

To avoid clogging the tribunals and courts with **low-value litigation**, the CBDT prescribes **monetary limits (measured by "tax effect")** below which the Department will **not** file or pursue an appeal. This is a deliberate **litigation-management** policy: officer time and court capacity are reserved for cases that matter, and small taxpayers are spared prolonged disputes.

The current limits — CBDT Circular No. 9/2024 dated 17.09.2024

Forum	Monetary limit (tax effect)	(Earlier limit)
ITAT (s.253)	**₹60 lakh**	(₹50 lakh)
High Court (s.260A)	**₹2 crore**	(₹1 crore)
Supreme Court (s.261 / SLP)	**₹5 crore**	(₹2 crore)

Key points: - The limits apply **both** to fresh appeals **and** to **pending** appeals — pending appeals below the enhanced threshold are to be **withdrawn**. - Crossing the limit does **not** compel an appeal: "an appeal should not be filed merely because the tax effect exceeds the limit" — the decision is still taken **on merits**. - **Exceptions** (from Circular 5/2024) let the Department appeal regardless of tax effect — e.g. where the **constitutional validity** of a provision is challenged, a Board **notification/circular** has been held illegal, or **TDS/TCS** and certain organised tax-evasion issues are involved.

e-Nivaran — integrated grievance redressal

What e-Nivaran is

What it is: e-Nivaran ("e-redressal") is the Income Tax Department's **Unified Grievance Management System**. It **consolidates grievances received across every channel** — the **e-Filing portal, CPGRAMS, CPC-ITR, CPC-TDS, ASK — Aaykar Seva Kendra (counter receipts) — and the Aaykar Sampark Kendra (call centre), NSDL/Protean, UTIITSL and SBI (Refund Banker)** — into a **single, tracked workflow**, so that one taxpayer complaint is monitored end-to-end under one identity instead of being handled in isolation across separate systems.

Why grievance redressal matters — to the taxpayer AND the Department

A grievance system is the *other* way (besides an appeal) that a citizen can get a wrong put right — used for service failures rather than legal disputes: a refund not received, a rectification not done, a demand wrongly shown, a return not processed.

- **Why it matters to the taxpayer:** a single, transparent, **24×7** channel to raise a problem and *see where it stands*, with a unique tracking number — no need to chase multiple offices. It reduces paperwork, delay and uncertainty.
- **Why it matters to the Department:**
- **Trust and legitimacy** — voluntary compliance depends on taxpayers believing the system will listen and fix mistakes.
- **Sevottam and the Taxpayers' Charter** — e-Nivaran is the measurable channel through which the Department delivers its Charter promises of *prompt, fair and courteous* service. e-Nivaran is in effect the **computerised integration of Sevottam** with grievance handling (ASK being the physical face of Sevottam).
- **Interoperability with CPGRAMS** — it syncs with the Government's central grievance portal to avoid duplication and keep updates aligned.
- **Management insight** — pendency, ageing and category-wise analysis of grievances tell supervisors where processes are failing, feeding back into better administration.

How a grievance is lodged, routed and resolved

- **Lodging:** the taxpayer files an e-Nivaran grievance **online on the e-Filing portal** (Grievances → Submit Grievance) or **manually at an ASK counter**; grievances from **CPGRAMS** flow in automatically. A **unique Grievance ID** is issued for tracking.

- **Routing / assignment:** the grievance is classified by **category and jurisdiction** and **assigned in ITBA (e-Nivaran module)** to the right authority — **AO / CPC-ITR / CPC-TDS / e-Filing / other**. It can be **transferred** between systems (e.g. AO ↔ CPC-ITR) when the issue belongs elsewhere, without the taxpayer having to re-file.
- **Resolution:** the assignee acts and, where relevant, links to the appropriate **ITBA functionality** — rectification u/s **154**, refund re-issue, return receipt/processing, demand correction. The action and reasons are recorded against the Grievance ID.
- **Monitoring:** the taxpayer **tracks status** with the Grievance ID; supervisory authorities monitor pendency, ageing and disposal for their charge.

ASK, Sevottam and the Taxpayers' Charter

- **ASK (Aaykar Seva Kendra): the single-window facilitation counter — distinct from the Aaykar Sampark Kendra (the call-centre channel) — that is** the physical embodiment of **Sevottam** and a **manual entry point** feeding e-Nivaran.
- **Sevottam:** the Government-of-India service-excellence framework (Citizen's Charter + grievance redress + service standards) that ASK and e-Nivaran together implement in the Income Tax Department.
- **Taxpayers' Charter (s.119A):** e-Nivaran operationalises the Charter's commitments — the concrete, trackable route through which the Department meets its promised service standards.

CPGRAMS — the Government-wide grievance portal (and how it connects to e-Nivaran)

What CPGRAMS is

What it is: CPGRAMS — the **Centralised Public Grievance Redress And Monitoring System** — is the **Government of India's single, online public-grievance portal**, run by the **Department of Administrative Reforms & Public Grievances (DARPG)** and reachable at **pgportal.gov.in** (also through the UMANG app). It is a **24×7** platform on which any citizen can lodge a grievance against **any** Central Ministry/Department or State — the Income Tax Department being **one department among all of them**. In other words, CPGRAMS is the *whole-of-government* complaint window; e-Nivaran is the ITD's *own* system for the grievances that concern it.

CPGRAMS vs e-Nivaran — how the two connect

The two must not be confused, though they are closely integrated: - **CPGRAMS** is **DARPG's government-wide** portal — a citizen uses it to complain about *any* department (tax, railways, pension, passport, etc.). - **e-Nivaran** is the **ITD's own Unified Grievance Management System** — it handles only income-tax grievances and links each one to the relevant ITBA action (rectification u/s 154, refund re-issue, demand correction, etc.). - **The link:** when a taxpayer's CPGRAMS grievance relates to income tax, CPGRAMS **auto-routes it to the concerned authority**, and it **flows into e-Nivaran** to be assigned and worked in ITBA. The disposal recorded in e-Nivaran is **synced back to CPGRAMS**, so the citizen sees the closure and status on whichever portal they used. This interoperability avoids duplicate handling and keeps the two systems' updates aligned. (e-Nivaran, recall, explicitly consolidates grievances received **from CPGRAMS** alongside its other channels.)

How a CPGRAMS grievance moves — lodging to disposal

1. **Lodging:** the citizen registers/logs in on **pgportal.gov.in**, selects the Ministry/Department and category, and submits the grievance (with attachments if any).
2. **Registration number:** the portal issues a **unique registration number** (a **UGRO-format** registration ID) with which the citizen **tracks status** throughout.
3. **Routing to the concerned officer:** the grievance is directed — increasingly by **AI-based auto-routing** — to the correct **Grievance Redressal Officer (GRO)** in the concerned department; for

income-tax matters this carries it to the appropriate ITD authority (and into **e-Nivaran** for action in ITBA).

4. **Disposal within the target time-limit:** under DARPG's **Comprehensive Guidelines dated 23 August 2024**, the prescribed redressal timeline was **reduced from 30 days to 21 days**, with an **interim reply** where more time is genuinely required.
5. **Feedback:** on closure, the citizen is intimated by **SMS and email**, and satisfaction is captured — including through a **feedback call centre**.
6. **Appeal to the Appellate Authority:** if **dissatisfied with the disposal**, the citizen may **file an appeal** within CPGRAMS to the department's **Appellate Authority** — an officer of **Additional/Joint Secretary** rank designated as the **Nodal Appellate Authority (NAA)** (with **Sub-Appellate Authorities** under them). The appeal is examined independently and is to be **disposed within 30 days**.

The CPGRAMS reform programme

CPGRAMS has been strengthened through a **"10-step reforms"** programme aimed at faster, higher-quality redressal. Its principal features are: **universalisation and AI-based auto-routing** of grievances to the right officer; **mapping of Grievance Redressal Officers**; a **structured multi-level appeal architecture** with feedback collected on every disposed grievance; **monitoring dashboards** (the "tree" dashboard and an intelligent grievance-monitoring dashboard) for **root-cause analysis**; and **language accessibility** (availability across scheduled languages). These reforms have enabled the Government to tighten the redressal target to **21 days** and to monitor departmental performance centrally.

Why CPGRAMS matters — to the taxpayer AND the Department

- **Why it matters to the taxpayer:** a **single window** to raise a tax grievance without knowing the ITD's internal structure — usable even by someone unfamiliar with e-Filing/e-Nivaran; a **unique registration number** to track it; a **defined time-limit** (21 days) for disposal; and a **built-in escalation** (appeal to the Appellate Authority) if the reply does not satisfy. It embodies **accountability and transparency** in dealing with government.
- **Why it matters to the Department:** CPGRAMS is a core instrument of **Sevottam** and the ITD's **service standards** — the external, government-wide mirror of the Charter promises that e-Nivaran delivers internally. Its **central monitoring dashboards** expose pendency, ageing and quality of redressal to DARPG and to CBDT, driving faster disposal and **process improvement**, and — like the right of appeal — it reinforces **taxpayer trust** by proving that complaints are heard, tracked and answerable up an independent appellate line.

Legal & procedural references

- **Income-tax Act, 1961:** s.246A (appealable orders); **s.249** (first appeal — Form 35, 30 days, fee); **s.250** (procedure in first appeal); **s.251** (powers of CIT(A)/JCIT(A) — confirm/reduce/enhance/annul); **s.253** (appeal to ITAT — Form 36, 60 days, by assessee or Department); s.260A (appeal to High Court on substantial question of law); s.261 (appeal to Supreme Court); s.154 (rectification, linked from e-Nivaran); s.119A (Taxpayers' Charter).
- **Faceless Appeal Scheme, 2021** — CBDT Notification No. **139/2021 dated 28.12.2021** (NFAC, appeal units, automated allocation, abolition of RFACs, VC personal hearing as a right); NFAC set up by Office Order dated 29.12.2021.
- **e-Appeals Scheme, 2023** — JCIT(Appeals) for small-demand appeals (Finance Act, 2023).
- **CBDT Circular No. 9/2024 dated 17.09.2024** — enhanced monetary limits for departmental appeals (ITAT ₹60 lakh / HC ₹2 crore / SC ₹5 crore); read with Circular 5/2024 (exceptions).

- **ITBA Appeal Register & CSR module** instructions; **ITBA e-Nivaran module** instructions; **Sevottam / Taxpayers' Charter** framework.

Key Takeaways

- The **right of appeal** is a taxpayer's core safeguard and a discipline on assessment quality. The appellate hierarchy, rising from fact to pure questions of law, runs:

1. CIT(A) / JCIT(A) — first appeal;
2. ITAT — second appeal;
3. High Court; and
4. Supreme Court.

- **First appeal: Form 35**, within **30 days** (s.249); powers of the CIT(A) to *confirm/reduce/enhance/annul* under **s.251**. **Second appeal to ITAT: Form 36**, within **60 days** (s.253) — available to **both** assessee and Department.
- **ITAT is the final fact-finding authority**; High Court and Supreme Court act only on a **substantial question of law**.
- **JCIT(Appeals)** was created by the **Finance Act, 2023** (e-Appeals Scheme, 2023) to clear **small-demand** first appeals.
- The **Faceless Appeal Scheme, 2021** is run by **NFAC**; it **abolished the Regional Faceless Appeal Centres**, uses **automated allocation direct to an appeal unit (CIT(A))**, and makes **VC personal hearing a right on request**.
- **CSR = Central Scrutiny Report** — the reasoned proforma scrutinising an adverse order to decide on a **further departmental appeal**; do **not** read it as "Register".
- CSR / departmental-appeal roles progress in the order:

1. AO;
2. Range Head; and
3. PCIT. For ITAT/HC matters, add **CIT(Judicial)** and **CCIT**; HC/SC filings are routed via the **Directorate of L&R**.

- The **Appeal Register** records receipt of appellate/judicial orders and **fixes the limitation date** for further appeal — the trigger for the CSR workflow.
- **Departmental-appeal monetary limits (Circular 9/2024): ITAT ₹60 lakh, HC ₹2 crore, SC ₹5 crore** (tax effect); apply to fresh **and** pending appeals; crossing the limit still requires a decision **on merits**; special exceptions apply.
- **e-Nivaran** is the **Unified Grievance Management System**, integrating **e-Filing, CPGRAMS, CPC-ITR, CPC-TDS, ASK, NSDL/Protean, UTIITSL and SBI**; it issues a **unique Grievance ID**, is assigned/resolved in **ITBA**, and delivers the **Sevottam / Taxpayers' Charter** service promise, building taxpayer trust.
- **CPGRAMS** (DARPG, **pgportal.gov.in**) is the **Government-wide** public-grievance portal — the ITD is one department on it; income-tax grievances **auto-route** to the concerned officer and **flow into e-Nivaran**, with disposal **synced back**. Target disposal **21 days** (DARPG guidelines, **23 Aug 2024**), with an **appeal** to the **Appellate Authority (NAA, Addl./Jt. Secretary rank; ~30 days)** — do **not** confuse CPGRAMS (whole-of-government) with e-Nivaran (ITD's own system).
- Module path: **ITBA Portal → Login → Modules → Appeal Register & CSR** (and the **e-Nivaran** module for grievances).

Key terms & abbreviations

- **CIT(A) / JCIT(A)** – Commissioner / Joint Commissioner (Appeals) — first appellate authorities.
- **ITAT** – Income Tax Appellate Tribunal (second appeal; final fact-finding authority).
- **NFAC** – National Faceless Appeal Centre (single point of contact under the Faceless Appeal Scheme).
- **RFAC** – Regional Faceless Appeal Centre (existed under the 2020 scheme; **abolished** in 2021).
- **Appeal Unit (AU)** – the CIT(A)-led team that decides a faceless appeal.
- **Appeal Register / Appeal Receipt Register** – ITBA record of appellate/judicial orders received, limitation and status.
- **CSR** – **Central Scrutiny Report** — scrutiny of an adverse order to recommend a further departmental appeal.
- **CIT (Judicial)** – authority that vets substantial questions of law for ITAT/HC appeals.
- **L&R** – Directorate of Legal & Research (handles HC/SC litigation coordination).
- **Form 35 / Form 36** – appeal forms to CIT(A)/JCIT(A) and to ITAT respectively.
- **Tax effect** – the measure of revenue at stake, compared against monetary limits for departmental appeals.
- **e-Nivaran** – Unified Grievance Management System of the Income Tax Department.
- **ASK – Aaykar Seva Kendra — single-window facilitation counter (face of Sevottam); distinguish the Aaykar Sampark Kendra (call centre).**
- **Sevottam** – Government service-excellence framework (Citizen's Charter + grievance redress + service standards).
- **CPGRAMS** – Centralised Public Grievance Redress And Monitoring System — DARPG's Government-wide public-grievance portal (**pgportal.gov.in**), interoperable with e-Nivaran; 21-day disposal target with appeal to the Appellate Authority.
- **DARPG** – Department of Administrative Reforms & Public Grievances — the Government's nodal department that owns and monitors CPGRAMS.
- **NAA / Appellate Authority (CPGRAMS)** – Nodal Appellate Authority (Addl./Jt. Secretary rank) who decides CPGRAMS appeals within ~30 days.
- **Taxpayers' Charter** – s.119A commitments on service standards that e-Nivaran/ASK operationalise.

Part V — Jurisdiction, Front Office & Information Systems

13. Jurisdiction and PAN / Case Transfer Functionality in ITBA

Applicable to: ITO Paper-V, ITI Paper-IV, MS Paper-IV (all three cadres)

Syllabus reference: ITBA Applications Modules — PAN/TAN: Transfer / Create Transfer Order, Bulk Transfer; jurisdiction over a taxpayer and its change in ITBA; Transfer of Cases (JAO ⇄ Faceless) in the Assessment module.

Overview

Every taxpayer in India is "owned" by one **Assessing Officer (AO)**. That ownership — who assesses the return, processes the refund, raises a demand, or takes recovery action — is what we call **jurisdiction**. In the Income Tax Business Application (ITBA), jurisdiction is stored against the PAN as an **AO Code**, and it is not permanent: PANs are re-assigned when offices are reorganised, when a search brings related cases together, or when a matter moves between the faceless and jurisdictional streams. This chapter first explains what jurisdiction is and why it matters, then sets out the four governing sections of the Income-tax Act, 1961 — **s.120, s.124, s.127 and s.129** — in plain language. It then describes, step by step, how a jurisdiction change is actually *executed* in ITBA: single and **Bulk PAN transfer** via **Create Transfer Order**, and the **Transfer of Cases** workflow (Faceless ⇄ JAO) documented in the ITBA *Transfer Functionality User Manual dated 11.06.2025*. Understanding both the *law* (the order) and the *system* (giving effect to it) is central to this topic.

What "jurisdiction" over a taxpayer means

What it is. Jurisdiction is the legal authority of a particular income-tax authority to deal with a particular taxpayer's affairs. When we say "AO Ward 3(2), Mumbai has jurisdiction over PAN ABCPK1234F", we mean that officer — and only that officer — is empowered to issue notices, frame the assessment, levy penalty, grant refunds and enforce demand for that PAN, for the years covered. Jurisdiction has several dimensions:

- **Territorial** — the geographical area (a locality, a set of PIN codes, a city).
- **Pecuniary** — income slabs (e.g. corporate charges vs non-corporate; "salary" ranges vs "business" ranges).
- **By class of person / income** — e.g. companies, trusts, international taxation, central charges (search cases), exemptions.

Why it matters to the taxpayer. A taxpayer must know *which* officer can lawfully act, where to file responses, and whom to approach. An order passed by an officer **without** jurisdiction is legally vulnerable. Jurisdiction also protects the taxpayer from being moved between officers arbitrarily — the law lets them object to a wrong AO (within limits) and gives a hearing before a transfer that causes real inconvenience.

Why it matters to the Department. Jurisdiction prevents two officers from acting on the same PAN, ensures every taxpayer is covered by exactly one accountable AO, and lets the Department distribute workload rationally (by area, income class, or specialisation such as search or international tax). Clean jurisdiction mapping is also what makes system-driven functions — CPC processing, refund banking, demand recovery, faceless allocation — work without collision.

The AO Code — how jurisdiction is stored in ITBA

What it is. The **AO Code** is a coded identifier of a jurisdiction. It is built from a top-down hierarchy:

1. **Region (RCC)**
2. **CCIT**
3. **CIT/PCIT**
4. **Range**
5. **AO (Ward/Circle)**

Each PAN in the system carries the AO Code of its current owning officer in the **PAN AO field**.

Why it matters. The AO Code is the technical "address" of the taxpayer inside every ITBA module. Changing that single field re-points the taxpayer's entire record — pending and disposed proceedings, the demand and refund ledger, e-proceedings and worklist items — to a new officer. In practical terms, **executing a jurisdiction change in ITBA = updating the AO Code on the PAN**. That is why "PAN transfer" and "jurisdiction change" are, operationally, the same act.

Jurisdiction — the legal framework

Four sections of the Income-tax Act, 1961 govern who owns a taxpayer and how ownership moves: **s.120** confers authority, **s.124** vests territorial jurisdiction and sets the objection deadline, **s.127** transfers a case, and **s.129** covers a mere change of officer in the same chair. Each is explained below, with the practical grounds for transfer and the taxpayer's hearing right in between.

Section 120 — Jurisdiction of income-tax authorities (the source of authority)

What it is. Section 120 is the foundational provision — the source of all jurisdiction. It says income-tax authorities shall exercise the powers and perform the functions **conferred on / assigned to them by the CBDT** through notifications. The CBDT (and, under delegated powers, the PCCIT/PCIT) issues **jurisdiction orders** specifying the area, the classes of persons, the classes of income and the cases each authority will handle.

Why it matters. Every AO's power to touch a taxpayer traces back to a s.120 notification. Without a s.120 vesting, an "AO" is not an AO for that case at all. When the Department reorganises charges — new ranges, new faceless units, corporate/non-corporate splits — it does so by fresh s.120 orders, which are then given effect in ITBA by re-mapping AO Codes (often through **Bulk Transfer**).

Section 124 — Jurisdiction of Assessing Officers (territorial vesting + the objection window)

What it is. Where an AO is vested (under s.120) with jurisdiction over an area, s.124 gives that AO jurisdiction over: - **(a)** persons carrying on a business or profession in that area (the *principal place* of business, if there are several); and - **(b)** any other person **residing** in that area.

The objection time-limit — s.124(3). A taxpayer who wants to *dispute* which AO has jurisdiction must do so **early**: where a return has been furnished — within one month of service of notice u/s 142(1) or 143(2), or before completion of the assessment, whichever is earlier; where no return has been furnished — within the time allowed by the notice u/s 142(1) or 148 for furnishing the return, or by the s.144 show-cause notice, whichever is earlier (s.124(3)). **Miss that window and the objection is barred forever.** Where there is a genuine dispute about who has jurisdiction, it is resolved by the **PDGIT/PCCIT/PCIT** (or the Board), not by the taxpayer's choice — s.124(2).

Why it matters. For the taxpayer, s.124(3) is a right that must be exercised within the time-limit or lost — a late-stage jurisdiction challenge to defeat an assessment usually fails. For the Department, s.124 gives a default rule for allocating fresh PANs (by residence / place of business) and a mechanism to settle jurisdiction disputes internally.

Section 127 — Power to transfer cases (the principal transfer power)

What it is. Section 127 is the specific power to **move a case from one AO to another**. The **PDGIT/PCCIT/PCIT (or DGIT/CCIT/CIT)** may transfer any case from an AO subordinate to that authority to another AO, subject to two mandatory conditions (the "**twin conditions**"):

1. **Reasonable opportunity of being heard** to the assessee, *wherever it is possible to do so*; and
2. **Recording of reasons** for the transfer.

Courts (e.g. Himachal Pradesh HC and others) have repeatedly held these twin conditions are **mandatory**, and — importantly — the reasons must be **communicated** to the assessee; it is not enough that reasons "exist in the file". A transfer order that merely states a conclusion without reasons is liable to be quashed for breach of natural justice (the principle that a person must be given a fair hearing before an adverse decision).

Not commonly subordinate — s.127(2). Where the transferor and transferee AOs are **not** subordinate to the same higher authority (e.g. an inter-city, inter-charge move), the **two superior authorities act in agreement**; if they cannot agree, the **Board (or a Board-nominated authority)** decides.

The same-city exception — s.127(3). If both AOs are in the **same city, locality or place**, **no opportunity of hearing is required** (the presumption being that the inconvenience is minimal). Reasons may still be recorded, but the hearing is dispensed with.

Any stage; no fresh notices — s.127(4). A transfer can be made at **any stage** of the proceedings, and it does **not** require the transferee AO to **re-issue** notices already validly issued by the transferor. The successor simply continues from where matters stand.

"Case" is defined broadly (Explanation to s.127). A "case" means **all proceedings under the Act** in respect of any year — **pending, completed, or that may be commenced** in future. So a s.127 transfer sweeps past, present and future years of that taxpayer to the new AO.

Why cases are transferred — and the taxpayer's right to be heard

Understanding *why* a transfer happens explains why the hearing right exists. Common grounds:

- **Search & seizure / centralisation.** After a s.132 search, related cases (the searched person, family, group companies, key employees) are pulled into a **Central Charge** so one investigation team handles the whole group coherently and can use seized material across cases.
- **Coordinated / group investigation.** Even without a search, connected assessees may be centralised so that inter-linked transactions are examined together and inconsistent findings are avoided.
- **Administrative convenience / workload balancing.** Reorganisation of ranges, creation of new charges, equalising pendency, or moving a case nearer to where records and the taxpayer actually are.
- **Change of address / place of business.** The taxpayer shifts city; the case moves to the AO of the new location.

The right to be heard (why it matters). A transfer — especially to another city or into a Central Charge — can cause real hardship: travel, new representation, and the consequences of centralisation. Section 127 therefore builds in **natural justice**: the assessee is told *why* and gets to *object* before the move (except same-city cases under s.127(3)). This is a genuine safeguard, and its breach is the single most common ground on which transfer orders are struck down. **A key practical point:** ITBA only *executes* the transfer by re-pointing the AO Code — the **s.127 speaking order** (an order that sets out its reasons), with reasons and hearing, is passed outside ITBA. The system records its reference; it does not supply the legal satisfaction of natural justice.

Section 129 — Change of incumbent (do NOT confuse with s.127)

What it is. Section 129 covers the situation where the **person holding an office changes** but the office (the AO Code) does not — e.g. the officer of Ward 3(2) is transferred/promoted and a new officer takes the same chair.

The **successor continues** the proceeding from where the predecessor left it. The assessee has a right to **demand a re-hearing** of matters already heard by the predecessor before the successor decides.

Why it matters / the distinction. - **s.127 = transfer of the *case*** — the **AO Code changes** (a different jurisdiction now owns the PAN). Requires reasons + hearing (subject to s.127(3)/(4)). - **s.129 = change of *incumbent*** — the **AO Code stays the same**; only the human officer changes. No transfer order; instead an optional re-hearing on demand.

In ITBA, a s.129 change is a **user/role remapping** to the *same* AO Code (handled through role administration), whereas a s.127 change is an actual **PAN transfer** to a *different* AO Code. Confusing the two is a common and consequential error.

Types of transfer in ITBA — an overview

Before turning to the mechanics, note the categories.

The three axes — charge relationship, volume, stream

Transfers differ along three independent axes: **who is subordinate to whom**, **how many PANs**, and **which stream** (jurisdictional vs faceless).

Axis	Category	Meaning
Charge relationship	**Intra-charge**	Source & destination AO under the **same PCIT/CIT** (often same Range/building). Frequently same-city → **no hearing** (s.127(3)).
Charge relationship	**Inter-charge / inter-station**	Source & destination under **different** CIT charges/stations. Needs s.127(1) order with hearing, or s.127(2) **agreement** between the two PCITs/CCITs if not commonly subordinate.
Volume	**Single PAN transfer**	One PAN re-pointed to a new AO Code.
Volume	**Bulk Transfer**	A **list of many PANs** moved in one transaction (reorganisation, restructuring, new-charge creation).
Stream	**Faceless ⇄ JAO**	*Pending proceedings* moved between the **Faceless/Assessment Unit** and the **Jurisdictional AO** via the Assessment-module Transfer of Cases workflow.

Two distinct ITBA functionalities — keep them distinct

There are **two different transfer mechanisms** in ITBA, and they must be kept apart:

1. **PAN transfer (PAN/AO functionality)** — changes the **AO Code on the PAN** itself. This migrates the *whole taxpayer record* (all years, ledgers, worklists). Screens: **Create Transfer Order**, **Bulk Transfer**. This is the ITBA execution of a **s.127** order.
2. **Transfer of Cases (Assessment module)** — moves a **single pending proceeding** (one PAN + one AY) between **Faceless (AU/FAO)** and **Jurisdictional AO (JAO)**, with an approval workflow. This is about the **faceless ⇄ jurisdictional stream** under **s.144B(8)**, not about re-owning the PAN wholesale.

PAN transfer — the PAN / AO functionality

The **PAN AO field** holds the AO Code that currently owns the PAN. Changing it is the technical act of jurisdiction transfer. Three routes exist depending on where the destination sits.

Single PAN transfer via Create Transfer Order

Within the same RCC/region, the PCIT/CIT (or an authorised officer) uses the **Create Transfer Order** screen. The steps are:

1. select the **source AO Code** and **destination AO Code**;
2. enter the **PAN(s)**;
3. record the **reason / order reference** (i.e. the particulars of the s.127 order); and
4. submit.

ITBA then generates a **Transfer Order** and updates the PAN's AO field. From that moment, the destination AO sees the taxpayer's proceedings and ledgers in its worklist.

Bulk Transfer of PANs

The same functionality supports moving **many PANs at once** — typically by selecting or uploading a structured/CSV list of PANs against a **destination AO Code**. This is the standard tool during **jurisdiction reorganisation, restructuring and new-charge creation**, where hundreds or thousands of PANs shift together (usually a same-city administrative move, so s.127(3) applies and no individual hearings are needed). System **validations** check that each PAN is active, is not already locked in a conflicting transfer, and that the destination AO Code is valid and active.

Inter-region / inter-charge transfer (request–accept)

Where the destination lies **outside the source PCIT's region**, the transfer runs as a **request–accept** workflow: the **source authority initiates** the transfer order and the **destination authority accepts** the PAN into its jurisdiction — the system reflection of the **s.127(2) agreement** between the two superiors. Until the destination accepts, the PAN may sit in an **"in-transit"** state, owned by neither side for new action.

> **Boundary of the system's role.** ITBA supports the *execution* of jurisdiction change (re-pointing the AO Code), **not** the legal satisfaction of natural justice. The s.127 speaking order — reasons, and hearing where required — is prepared and served **outside** ITBA; the system merely records its reference and gives it effect.

Transfer of Cases functionality (Assessment module) — per the ITBA User Manual (11.06.2025)

This is the second, distinct mechanism. Per the *Transfer Functionality User Manual dated 11.06.2025*, it "facilitates the users to transfer the **pending proceedings** from Assessment Unit to JAO or vice-versa … with the approval workflow in ITBA." It is **currently available in the Assessment module**.

Why this exists — the faceless ⇄ jurisdictional interface

What it is. Under **s.144B**, most scrutiny assessments are done **faceless** by the **National Faceless Assessment Centre (NaFAC)** through **Assessment Units (AU/FAO)** allotted by an **automated random allocation** system — the taxpayer never meets the officer. But some cases must leave the faceless stream (e.g. **s.144B(8)**: the PCCIT/PDGIT in charge of NaFAC may, **with prior CBDT approval**, transfer a case to the **JAO** having jurisdiction). Conversely, cases sometimes need to be brought into faceless.

Why it matters. This functionality is the interface between the two regimes. Getting it right ensures that when a case moves, the **JAO takes into account the proceedings already conducted** under faceless (notices issued, replies filed) and continues — consistent with **s.127(4)** (no re-issue of notices) and the CBDT procedure for cases transferred out of faceless.

Login & navigation

To reach the screen:

1. Go to https://itba.incometax.gov.in and select **Login Here** (enter User Name, Password, OTP).
2. Open *Modules → Assessment*.

3. Select *Menu → Transfer of cases (JAO ⇄ FAO)*.
4. Choose **Transfer Out Cases** (or **Transfer by NaFAC** for the NaFAC role).

Allocation type — Original vs Transferred (this decides the workflow)

What it is. Every proceeding carries an **allocation type**: - **Original Allocation** — the proceeding has **never** been moved via this Transfer functionality before. - **Transferred Case** — the proceeding has been moved **at least once** via this functionality.

Why it matters. The allocation type **determines whether an approval workflow is required or not** for a given direction. This is the single most important variable in the five scenarios below — read each scenario with the allocation type in mind.

Common initiation steps (Transfer Out Cases screen)

1. Enter **PAN (mandatory)** and **AY (mandatory)**.
2. **Proceeding Type** is auto-set by the module.
3. Click **Search** → pending proceedings are listed. **Only one proceeding can be transferred at a time.**
4. Select the proceeding, choose the **Case Type** (based on the logged-in user), enter **Proposal Remarks**.
5. Optionally add **Attachments** (select **Category**, enter **Description**, choose file, **Upload**).
6. Click **Submit** (workflow cases) or **Transfer** (direct cases). A success message confirms; where a workflow applies, a **proposal workitem** is created for the next authority.

The five scenarios (workflow depends on direction + allocation type)

Scenario 1 — AU(AO) → JAO, Original Allocation. Approval workflow required. The proposal moves through:

1. **FAO** initiates the transfer proposal;
2. **FRange Head** records a **Recommendation** and **Workflow Notings**, then submits; and
3. **FPCIT** either **rejects** at own level, or **approves only after offline NaFAC approval** — capturing the **Date of offline approval by NaFAC**, the **Offline File Reference No. of NaFAC**, and **Remarks/Workflow Notings** (all **mandatory**).

On approval, the proceeding moves to the JAO.

Scenario 2 — AU(AO) → JAO, Transferred Case. The **same** approval workflow as Scenario 1 (FAO, then FRange Head, then FPCIT).

Scenario 3 — JAO → AU(AO), Original Allocation. Direct — no workflow. The JAO:

1. enters **PAN & AY**;
2. selects the **Case Type**;
3. enters **Proposal Remarks**; and
4. clicks **Transfer**.

The request is queued after a confirmation message. No approval is needed.

Scenario 4 — JAO → AU(AO), Transferred Case. Approval workflow required. The proposal moves through:

1. **JAO** initiates the transfer proposal;
2. **J.Range Head** records a **Recommendation** and **Notings**, then submits; and
3. **JPCIT** either **rejects**, or **approves after offline NaFAC approval** (same mandatory fields as Scenario 1).

On approval, the proceeding moves to the FAO.

Scenario 5 — Transfer by NaFAC. Direct — no workflow. The NaFAC AO moves cases **Faceless ⇄ Non-Faceless** for **any** allocation type:

1. enter **PAN & AY**;
2. choose the **Proceeding Category** (Faceless / Non-Faceless);
3. select the **Case Type**;
4. enter **Proposal Remarks**; and
5. click **Transfer**.

In summary: an **approval workflow (Range → PCIT)** is required only when a case is going **out of** the faceless stream (or back and forth) for the more sensitive combinations — **AU→JAO (both allocation types)** and **JAO→AU when already a Transferred Case**. **JAO→AU Original** and **any NaFAC transfer** are **direct, no-workflow** actions. And every workflow approval (FPCIT/JPCIT) is gated on **offline NaFAC approval** being captured — reflecting the CBDT requirement of prior approval to move cases out of faceless.

Workflow controls — send-back, reject, approve

- **Send Back for Clarification.** At each stage the higher authority (Range) can **Send Back** the workitem with *Action Required = Clarification Sought*. The initiating AO can then **Cancel** the proposal or **Re-submit** after providing clarification (Workflow Notings entered at each step).
- **Reject.** The PCIT/JPCIT can **Reject** (Workflow Notings mandatory); rejection **closes** the proposal workitem.
- **Approve.** The PCIT/JPCIT approves after entering the mandatory NaFAC offline-approval fields; the proceeding then transfers to the destination jurisdiction.
- **Proposal Workitem.** A **proposal workitem** appears in the next authority's **Assessment Worklist**, exposing **Proposal Details**, **Case History/Notings**, and **Attachments** contributed by earlier users.

Effect on the pending proceeding & how it is carried

Consistent with **s.127(4)**, the transfer is valid at any stage and **no notice already issued is re-issued**. ITBA carries the proceeding — **with its full history/notings** — into the destination officer's worklist, where the receiving AO/AU can open the workitem and continue (and review everything the previous side did).

Restoration / reversing a wrong transfer

A wrongly-routed case is **restored by initiating a transfer in the reverse direction** — e.g. Scenarios 3/4 reverse Scenarios 1/2 — or by NaFAC reversing a NaFAC transfer.

The NaFAC lock — an important restriction

Per the manual's "Important Note": once a case has been transferred by a **NaFAC** user, the **FAU or JAO cannot** raise a fresh transfer proposal on that case. If they want it moved again, they must send an **offline proposal to NaFAC**, and **only NaFAC** can then act. This prevents field officers from undoing a centrally-controlled (NaFAC) routing decision on their own.

User roles & screen access (from the manual)

User	Key screens
Assessment Unit (AO) / JAO	Transfer of Cases screen; Assessment Worklist; 143(3) Workitem; List/View of Notices–Orders–Letters
AU Range Head / J.Range	Transfer Proposal workitem; Assessment worklist; Status Monitor
AU PCIT / J.PCIT	Transfer Proposal workitem; Assessment worklist; Status Monitor
NaFAC AO	Transfer by NaFAC; Assessment worklist

Legal & procedural references

- **Income-tax Act, 1961: s.120** (jurisdiction of income-tax authorities — CBDT notifications); **s.124** (jurisdiction of AOs; territorial vesting; **s.124(3)** bar on belated objection); **s.127** (power to transfer cases — twin conditions of hearing + recorded reasons; **s.127(2)** agreement where not commonly subordinate; **s.127(3)** same-city exception; **s.127(4)** any-stage transfer, no re-issue of notice; Explanation defining "case"); **s.129** (change of incumbent of an office); **s.139A** (PAN); **s.144B** (faceless assessment; **s.144B(8)** transfer to JAO with prior CBDT approval).
- **ITBA source:** *Transfer Functionality User Manual, dated 11.06.2025* — Assessment-module Transfer of Cases, Scenarios 1–5, user roles.
- **CBDT:** jurisdiction orders/notifications u/s 120 defining AO Codes and charge structure; CBDT procedure for cases transferred out of faceless assessment/penalty to the JAO.

Key Takeaways

- **Jurisdiction = which AO lawfully owns a taxpayer.** In ITBA it lives in the **PAN AO field / AO Code** (Region, CCIT, PCIT, Range, AO). Changing the AO Code *is* the transfer.
- **Four sections, four roles: s.120** confers authority (CBDT notifications); **s.124** vests territorial jurisdiction and sets the **objection deadline (s.124(3))**; **s.127** transfers a case; **s.129** covers a mere change of officer in the same chair.
- **s.127 twin conditions are mandatory: reasonable opportunity of being heard** + **recorded (and communicated) reasons** — breach = order liable to be quashed for violating natural justice.
- **s.127 exceptions: same city/locality/place → no hearing (s.127(3))**; transfer at **any stage** and **no re-issue of notices (s.127(4))**; **not commonly subordinate → agreement of the two superiors (s.127(2))**.
- **Do not confuse s.127 with s.129:** s.127 **changes the AO Code**; s.129 keeps the **same AO Code**, only the incumbent changes (with a right to demand re-hearing).
- **Why transfers happen:** search/centralisation, coordinated investigation, administrative convenience, change of address — the hearing right exists because transfers can genuinely burden the taxpayer.
- **Two distinct ITBA tools:** (1) **PAN transfer** — *Create Transfer Order* / **Bulk Transfer** re-owns the whole PAN (executes s.127); (2) **Transfer of Cases (Assessment module)** — moves **one pending proceeding** between **Faceless (AU/FAO)** and **JAO** under s.144B.
- **Bulk Transfer** moves many PANs in one transaction (reorganisation/new charges), with validations on PAN status and destination AO Code; inter-region moves use a **request–accept ("in-transit")** flow reflecting s.127(2).
- **Allocation type drives the workflow: Original** vs **Transferred Case** decides whether Range→PCIT approval is needed. **AU→JAO (both types)** and **JAO→AU (Transferred)** need workflow; **JAO→AU (Original)** and **all NaFAC** transfers are **direct, no workflow**.

- **Only one proceeding at a time** (PAN + AY mandatory); FPCIT/JPCIT approval is **gated on offline NaFAC approval** (Date + Offline File Reference No. mandatory) — mirroring CBDT's prior-approval requirement to exit faceless.
- **NaFAC lock:** once NaFAC transfers a case, the FAU/JAO **cannot** re-propose a transfer — they must send an **offline request to NaFAC**.
- **ITBA executes, it does not adjudicate:** the s.127 speaking order (reasons + hearing) is passed **outside** ITBA; the system only records its reference and re-points the AO Code.

Key terms & abbreviations

- **AO Code** — coded jurisdiction identifier (Region/CCIT/CIT/Range/AO) attached to a PAN.
- **PAN AO field** — the ITBA field holding the current owning AO of a PAN.
- **Create Transfer Order** — ITBA screen to generate a PAN transfer order (single or bulk).
- **Bulk Transfer** — moving multiple PANs to a destination AO Code in one transaction.
- **JAO** — Jurisdictional Assessing Officer; **FAO / AU(AO)** — Faceless / Assessment Unit AO.
- **NaFAC (formerly NeAC) — National Faceless Assessment Centre (distinguish NFAC — the National Faceless Appeal Centre, Chapter 12).**
- **Allocation type** — *Original Allocation* vs *Transferred Case*; determines the workflow.
- **Proposal Workitem** — workflow item created in the next authority's Assessment Worklist to approve a transfer.
- **Intra-charge / Inter-charge** — transfer within the same CIT charge vs across charges/stations.
- **In-transit** — state of a PAN whose inter-region transfer has been initiated but not yet accepted by the destination.
- **Twin conditions (s.127)** — opportunity of being heard + recorded reasons.
- **Change of incumbent (s.129)** — new officer, same AO Code; assessee may demand re-hearing.

14. AIMS and Aaykar Seva Kendra (ASK)

Applicable to: ITO Paper-V, ITI Paper-IV, MS Paper-IV (all three cadres).

Syllabus reference: ITBA Application Modules (general) + departmental front-office / taxpayer-service systems — the AIMS module and the Aaykar Seva Kendra (ASK) single-window receipt system within ITBA; the Sevottam service-quality framework and the Citizen's / Taxpayers' Charter.

Overview

This chapter covers two ITBA modules that sit on opposite sides of the Department's relationship with the taxpayer. **AIMS** is a *back-office* module used only by officers: it pushes pre-identified, "actionable" information (non-filers, penny-stock transactions, potential prosecution cases) to the Assessing Officer, who verifies it and, where warranted, initiates proceedings such as reopening under section 148. **ASK** (Aaykar Seva Kendra) is the *front-office* single-window facility where taxpayers physically submit returns, applications, letters (DAK) and grievances, receive a system-generated acknowledgement on the spot, and have the item routed into the correct departmental workflow. ASK operates under the Government of India's **Sevottam** service-quality framework and gives effect to the Income Tax Department's **Citizen's / Taxpayers' Charter**. Taken together, the two modules reflect the Department's dual role: a data-driven *enforcer* (AIMS) and a citizen-centric *service provider* (ASK).

PART A — AIMS (Actionable Information Monitoring System)

AIMS: concept, purpose and the case types loaded

What AIMS is (concept explainer)

AIMS is an ITBA module that lets officers **view selected, pre-flagged cases** and **initiate necessary action** on any of them. The cases are not chosen by the officer at random; they are **centrally uploaded** based on information already available with the Department (from the Non-filers Monitoring System, financial-transaction data, market-manipulation analysis, and so on). In effect, AIMS is a structured list of leads that the system has flagged for closer examination, presented to the jurisdictional officer inside a secure, auditable environment.

Why actionable-information monitoring matters

The Department collects vast quantities of third-party and transactional data. Data by itself does nothing — its value is realised only when a specific officer examines a specific case within a specific time and records an outcome. AIMS exists to close that gap. It enables **verification and monitoring of actionable information in a secure manner**, converting raw information into **time-bound, traceable field action** rather than allowing leads to remain unactioned.

- **To the Department:** it improves *coverage and accountability* — every lead has an owner, a status and an audit trail; supervisors can see what is pending, under verification or closed, and disposal can be measured through MIS reports. It also standardises how information becomes assessment or prosecution, reducing arbitrariness.
- **To the taxpayer:** it means action is *evidence-led and consistent* — a case is opened because concrete information exists, and the taxpayer is given an opportunity to respond (via letters) before any proposal to reopen is initiated.

The four AIMS case types (what is loaded)

Data for the following case types have been loaded into AIMS:

Case type in AIMS	Nature
Non-filers under **NMS** (Non-filers Monitoring System)	Persons with information of income/transactions but **no return** on record
Penny stock transactions	Suspected bogus LTCG/STCG through manipulated / low-value scrips
Potential prosecution cases u/s **276C(2)**	Wilful attempt to **evade payment** of tax
Potential prosecution cases u/s **276CC**	**Failure to furnish** return of income

The list is extensible — the module is designed so that “various case types **may** be uploaded” over time; the four above are the currently loaded set.

AIMS access: users, login and the dashboard

Who can use AIMS — users and access

AIMS is a **restricted, internal** module. It is available to the **Assessing Officer (AO) and officers above the AO**. All AOs can view the list of cases of each case type for a given **financial year, status and priority**. The **Actionable Information Monitoring System** link sits under the Menu, available to *AO and above*. The menu also exposes **MIS Reports** (View Reports) and **Help & FAQs / online training**. There is no taxpayer-facing side to AIMS.

Logging in to the AIMS module (officer workflow)

1. Navigate to the ITBA portal https://itba.incometax.gov.in and click **“Login Here”**.
2. Enter **Username, Password and RSA** token, then click **Login**.
3. On the portal home page, under **MODULES**, click **AIMS**. The AIMS Module home page opens.
4. From the **Quick Links** on the AIMS home page, open the **Actionable Information Monitoring System dashboard**.

The AIMS Dashboard and the three case statuses

The **AIMS Dashboard Screen** displays, for the logged-in officer (auto-populated by default from the login), the **count of cases** in each status, for each case type and financial year. On the dashboard the officer selects **Case Type, Financial Year and Priority** in the search criteria and clicks **Search**. Each status count is a **hyperlink**; clicking it opens the **AIMS List View** of the underlying cases.

The three statuses are central to the entire module:

Status	Meaning
Pending for initiation	Case loaded but officer has not yet started verification/action
Under verification	Officer has begun examining the information / issued a letter
Closed	Action concluded — verified with no further action, or a proposal initiated

A case normally moves through three stages: 1. **Pending for initiation**; 2. **Under verification**; and 3. **Closed**.

Working a case in AIMS: List View and Case View

AIMS List View — selecting and bulk-processing cases

Clicking a hyperlinked status count opens the **AIMS List View Screen**, which lists all cases under the chosen case type / FY / status / priority. Search fields are auto-populated except **PAN**; the officer may enter a valid PAN to filter to one taxpayer. From the list view the officer can: - Click **View** against a case to open the **AIMS Case View**. - Select multiple cases via the left-side **check boxes** and use **Bulk Letter Generation** to issue letters to many assessees at once. - Retrieve generated letters via **Menu → View/Download Notice/Letter/Order**.

AIMS Case View — the actions available on a single case

The **AIMS Case View Screen** is the detailed view of one case and the workbench for all actions:

- **Edit communication / email address.** Update the assessee’s address or email **before** issuing a letter, so the communication reaches the right place.
- **Select Other Activity.** Choose an activity from the drop-down, enter **Remarks**, and click **Confirm**. The activity is then logged in the **Activity Tracker** on the same screen — creating the audit trail.
- **Generate Letter.** Click **Generate Letter** to open the AIMS Letter screen; enter the required details, click **Generate**, confirm, and download via the *“Download File here”* hyperlink (also stored under **Menu → View/Download Notice/Letter/Order**). This is the officer’s primary means of seeking the taxpayer’s explanation.
- **Initiate Proposal for Issue 148.** This is the key output of AIMS. Clicking **Initiate Proposal for Issue 148** opens the **Selection of Cases for Scrutiny** screen, with **Notice u/s auto-populated as 148** and Name / PAN / AY already filled in. The officer then:

1. clicks **Record Reason** and **Select Reason**;
2. enters the **basis of selection**;
3. clicks **Proceed**; and
4. clicks **Submit** to initiate the reopening proposal.

- This is how AIMS feeds *directly* into the assessment stream.
- **Attachments.** Upload supporting documents, the **response received from the assessee**, or others — each with a category and description, then **Upload**.
- **Assessee Communication History.** Opens the **Case History / Noting** screen (PAN/TAN and history auto-populated). The officer enters remarks against a noting and clicks **Save**, building the case record.

Supporting grids on the Case View — the full context

Two read-only grids give the officer context before acting: - **Information Summary** grid: **Info-code**, information description, and the **number and value** of the underlying information. - **Related Cases (Same PAN)** grid: all *other* AIMS information for the same PAN — case type, FY, status, activity count and tax collection — so the officer sees the taxpayer's full AIMS footprint, not just the one lead.

An **AIMS Activity Report** and MIS reports let supervisory officers monitor progress and disposal across the charge.

How AIMS feeds into assessment and prosecution

AIMS is the **bridge between *information and assessment***. The officer verifies the flagged information (letters to the assessee, examining responses), records the outcome, and where escapement is indicated, **initiates a section 148 proposal** straight from the case — pushing it into the regular / faceless reassessment stream under sections **147–151** (with the section **148A** enquiry-and-opportunity procedure) and, for the assessment itself, section **144B**. For **non-filers** it prompts return-enforcement; for **276C(2) / 276CC** cases it supports a **prosecution** decision. The status then moves to **Closed**, leaving a complete audit trail in the Activity Tracker.

PART B — Aaykar Seva Kendra (ASK)

ASK: concept and why a single-window front office matters

What ASK is (concept explainer)

The **Aaykar Seva Kendra (ASK)** is the Department's **single-window front office** for the receipt of **returns, applications, letters (DAK) and grievances**. A taxpayer (or representative) can submit an item **in person or through a drop-box**, and receives a **system-generated unique acknowledgement number on the spot**. Within ITBA, ASK is a dedicated module that captures each receipt and routes it as a work-item to the correct officer's worklist. In summary, **ASK is the single-window system for implementation of the Citizen's Charter of the Income Tax Department.**

Before ASK, a taxpayer often did not know *where* to hand in a paper, *whether* it had been received, or *when* it would be dealt with. ASK addresses all three.

Why it matters to the taxpayer

- **Ease / single point of contact** — one counter accepts returns, applications, letters and grievances; no running between rooms.
- **Certainty of receipt** — a **token / acknowledgement number** is generated immediately, proving *what* was submitted and *when*. For a DAK, an **acknowledgement e-mail** is also sent automatically.
- **Transparency / trackability** — the acknowledgement number lets the taxpayer **track status** later (Search DAK / Search Return), and the Citizen's Charter timelines tell them *when* to expect action.

Why it matters to the Department

- **Sevottam and service standards** — ASK is the delivery vehicle for the Department's promised, time-bound service standards; it operationalises the shift from a pure *enforcement* agency to a *service provider*.

- **Pendency control and accountability** — every receipt becomes a monitored work-item with an owner and a status, so no item goes untracked, and supervisors can measure timeliness.
- **Clean routing** — items land in the *right* ITBA module (AST, e-Nivaran, the assigned officer's worklist) automatically.

The service-quality foundation: Sevottam and the Charters

The Sevottam framework (concept explainer)

Sevottam ("**Seva**" + "**Uttam**" = excellence in service delivery) is the citizen-centric service-quality framework promoted by the Department of Administrative Reforms & Public Grievances (DARPG), aligned to Bureau of Indian Standards standard **IS 15700:2005**. ASK centres adhere to these service-quality standards, and ASK is the mechanism CBDT uses to implement the Sevottam philosophy. Sevottam rests on **three pillars**:

Sevottam pillar	In the Income Tax Department
Citizen's Charter	Declares the services offered and the **time-limits** for each
Public Grievance Redress	Time-bound handling of grievances (ASK + **e-Nivaran** + **CPGRAMS**)
Service Delivery Capability / Enablers	Training, infrastructure and process reforms underpinning ASK

The Citizen's / Taxpayers' Charter link (concept explainer)

The Charter is the *promise* that ASK is built to deliver.

- **Citizen's Charter (the Sevottam pillar).** The Department reviewed its **1998** Citizen's Charter as the first step towards Sevottam; a new Charter with specific service **timelines** was finalised in **March 2007**, reviewed in **2010**, and revised again as the **Citizen's Charter 2014** (released 29 April 2014). It declares the services offered and the time-limit for each (e.g., indicative norms for issuing refunds and disposing of applications / grievances) — and **ASK is the single-window through which those commitments are fulfilled**.
- **Taxpayers' Charter (statutory, 2020).** Separately, section **119A** of the Income-tax Act (inserted by the Finance Act, 2020) empowered the CBDT to adopt a **Taxpayers' Charter**, notified with effect from **13 August 2020**. It sets out the Department's **commitments** to the taxpayer (to be fair, courteous and reasonable; to treat the taxpayer as honest; to provide a fair appeal/review mechanism; to maintain confidentiality; to decide matters in a time-bound manner; to publish service standards) and the taxpayer's **obligations** (to be honest and compliant, keep records, know what the representative does, respond in time, and pay on time).

> For the candidate: the **Citizen's Charter** is the *Sevottam/service-standards* document that ASK operationalises; the **Taxpayers' Charter 2020 (s.119A)** is the *statutory rights-and-obligations* document. Both express the same service-provider ethos; ASK is where it becomes tangible at the counter. Charter service timelines fall within the Taxpayer Services paper and are not examinable here.

Using the ASK module: users, login and receipts

Users of the ASK module

Role	Function
Front Desk	Receives DAK/returns over the counter, captures details, issues acknowledgement
Back Desk	Internal handling / movement of received items
Data Entry Operator (DEO)	Data entry of receipts
AO and above	Work on / resolve DAK; act on grievances; take substantive action

Logging in to the ASK module

Open https://itba.incometax.gov.in, enter **User ID, Password and RSA**, click **Login**; under the **Modules** tab click **ASK** to open the ASK home page.

Receiving a DAK / grievance

- Open the **DAK Receipt Form**, enter the DAK details, click **Save**.
- A **pendency / work-item** is created in the **"Assigned to" officer's worklist**. For **grievances**, the work-item is created in the **e-Nivaran** module worklist for action.
- An **acknowledgement e-mail** is sent automatically to the assessee on receipt of the DAK.

Receiving a return

- Open the **Return Receipt Form**, enter the return details, click **Save**.
- A pendency is created for the Jurisdiction Officer, and the return flows to the ITBA ITR-Processing module for processing.
- *Context:* today most returns are e-filed and processed centrally at **CPC** under section **143(1)**; the ASK return-receipt path handles **paper / over-the-counter** returns and related documents.

Tracking status (DAK and Return)

- **Search DAK** — enter the search criteria and click **Search**; results show the DAK with its **latest status**.
- **Search Return** — search by **PAN** *or* **Acknowledgement Number**; results show the return with its latest status.

The acknowledgement number is the single thread the taxpayer uses to follow an item end-to-end.

Resolving a DAK and integrating with departmental workflow

Working on / resolving a DAK (AO & above)

- From the **DAK Pendency List**, enter the search criteria, **Search**, and click the **Acknowledgement Number** hyperlink to open **DAK Details**.
- On **DAK Details** the officer can **View / Edit and Save**, **Add Attachments**, **View History of DAK**, **Issue / Generate a letter** to the assessee, **Re-assign** the DAK to another user, **Initiate Action** with the integrated modules, and finally **Resolve** the DAK.

Other actions in ASK

Transfer of Physical Records, printing of **Pre-printed ASK Acknowledgement Slips**, and **Bulk Receipt of Returns** — all available to Front Desk, Back Desk, DEO and AO & above.

How ASK integrates with departmental workflow

ASK is not a standalone counter — every receipt becomes a **work-item** in the relevant ITBA module: - **Returns → ITBA ITR-Processing module (jurisdictional AO / CPC processing). - Grievances → e-Nivaran** worklist (and onward to **CPGRAMS** where applicable). - **Applications / letters (DAK)** → the assigned officer's pendency for action and resolution.

The unique acknowledgement number issued at receipt is the thread that lets both the taxpayer (status tracking) and the Department (pendency monitoring) follow the item end-to-end — operationalising the Sevottam promise of transparent, time-bound service.

Legal & procedural references

- **Sections 147–151, IT Act 1961** — income escaping assessment / reopening via **notice u/s 148** (the AIMS "Initiate Proposal for Issue 148" output); **section 148A** enquiry-and-opportunity procedure and **section 144B** (faceless) for the downstream assessment.
- **Sections 276C(2) and 276CC** — prosecution for wilful attempt to evade payment of tax, and failure to furnish return — the prosecution case types in AIMS.
- **Section 139 / 139A** — return filing and PAN, underlying NMS non-filer cases.
- **Section 143(1)** — processing of returns (CPC), relevant to ASK return-receipt.
- **Section 119A** — statutory basis for the **Taxpayers' Charter** (inserted by Finance Act 2020; Charter notified 13 August 2020).
- **NMS** (Non-filers Monitoring System) — source of AIMS non-filer cases.
- **Sevottam framework** (DARPG) and **IS 15700:2005** (BIS); the Income Tax Department's **Citizen's Charter** (1998 → 2007, revised 2010 and 2014).
- **e-Nivaran** grievance module and **CPGRAMS** — grievance-redress integration.

Key Takeaways

- **AIMS = Actionable Information Monitoring System**; a *back-office*, officer-only module for **AO and above** — it is **not** taxpayer-facing.
- AIMS turns collected information into **time-bound, auditable action**: its four loaded case types are **NMS non-filers, penny-stock transactions, s.276C(2) and s.276CC** potential prosecution cases.
- The three AIMS dashboard **statuses** are **Pending for initiation**, **Under verification** and **Closed**; each count is a hyperlink into the List View.
- AIMS feeds assessment through **"Initiate Proposal for Issue 148"** — the Selection-of-Cases screen auto-populates **Notice u/s 148**, pushing the case into the s.147–151 / 144B reassessment stream; it also supports **prosecution** for 276C(2)/276CC and return-enforcement for non-filers.
- **ASK = Aaykar Seva Kendra**, the **single-window front office** that issues a **system-generated acknowledgement on the spot**; submissions allowed **in person or by drop-box**; it is *the single-window for implementing the Citizen's Charter*.
- ASK matters to the **taxpayer** (ease, token/acknowledgement, transparency, trackability) and to the **Department** (Sevottam service standards, pendency control, clean routing) — reflecting the Department as a **service provider**, not only an enforcer.
- **Sevottam** ("Seva + Uttam", IS 15700:2005) rests on three pillars: **Citizen's Charter, Public Grievance Redress, Service Delivery Capability**.
- Distinguish the **Citizen's Charter** (Sevottam service-standards document, 2007/2010/2014) from the statutory **Taxpayers' Charter 2020** under **section 119A** (rights, obligations and Department commitments).

- In ASK routing: a **DAK** creates pendency for the **"Assigned to" officer**; a **return** creates pendency for the **Jurisdiction Officer** and appears in **AST**; **grievances** route to **e-Nivaran** (→ CPGRAMS).
- Login to both modules needs **Username/User ID + Password + RSA** at https://itba.incometax.gov.in, opened from the **MODULES** tab; **track a DAK by acknowledgement number** and a **return by PAN or Acknowledgement Number**.

Key terms & abbreviations

- **AIMS** — Actionable Information Monitoring System (ITBA module; officer-only).
- **ASK** — Aaykar Seva Kendra (single-window taxpayer front office).
- **DAK** — letter / correspondence / application received at the counter.
- **NMS** — Non-filers Monitoring System.
- **AST — the legacy Assessment Information System (see Chapter 01); current returns are processed in the ITBA ITR-Processing module.**
- **RSA** — RSA secure token for ITBA login.
- **DEO** — Data Entry Operator.
- **Sevottam** — Government of India service-quality framework (Seva + Uttam; IS 15700:2005).
- **Citizen's Charter** — Department's declared services and service timelines (Sevottam pillar).
- **Taxpayers' Charter** — statutory charter of rights/obligations under section 119A (2020).
- **e-Nivaran** — ITBA / e-filing integrated grievance-redress module.
- **CPGRAMS** — Centralised Public Grievance Redress and Monitoring System.
- **CPC** — Centralised Processing Centre (return processing under s.143(1)).
- **MIS** — Management Information System (reports).

15. Insight Application Module, Project Insight and the e-Verification Scheme, 2021

Applicable to: ITO Paper-V, ITI Paper-IV, MS Paper-IV (all three cadres).

Syllabus reference: Insight application module — Introduction; Data Handling in Insight; Process Flow of Insight; E-verification; Third Party Reporting.

Overview

Modern tax administration in India has shifted from **intrusive enquiry** (summons, surveys, physical scrutiny of a few) to **data-driven, non-intrusive compliance** — using information the Department already receives from third parties to nudge the many towards voluntary compliance. **Project Insight** is the technology backbone of this shift: it is the Income Tax Department's integrated **Data Warehousing & Business Intelligence (DW&BI)** platform. It ingests billions of financial data points from banks, sub-registrars, mutual funds, employers and foreign jurisdictions, links them to a single taxpayer view keyed on PAN, risk-scores the anomalies, and drives outreach and case selection. This chapter explains what Project Insight is and why it matters, the **Annual Information Statement (AIS)** and **TIS** it powers, the **third-party reporting (SFT)** regime that feeds it, and the **e-Verification Scheme, 2021** (notified under **section 135A**) through which return–information mismatches are resolved online — the softest touch before any scrutiny or reassessment.

What Project Insight (the Insight portal) is

Project Insight is an integrated platform for **data warehousing, data mining, analytics and compliance management** rolled out by the Directorate of Income Tax (Systems), CBDT, in phases; the original operations phase concluded on 31 March 2025, and Insight 2.0 commenced on 1 April 2025. Its three stated objectives are: 1. **Promote voluntary compliance and deter non-compliance.** 2. **Impart confidence** that all eligible persons pay the appropriate tax. 3. **Promote a fair and judicious tax administration.**

Insight is not a single website but a family of channels: - The **Insight portal** (insight.gov.in) — the **officer-facing** analytics and case-management workbench, where AOs and investigation units see information, risk scores and cases. - The **Reporting Portal** (report.insight.gov.in) — where **reporting entities** (banks, registrars, etc.) register and file statements such as Form 61A. - The **Compliance Portal** (compliance.insight.gov.in / ais.insight.gov.in, reachable through the e-filing site) — the **taxpayer-facing** window for AIS, e-campaigns and e-verification responses.

Why data-driven, non-intrusive compliance matters

- **To the taxpayer:** most interactions become **faceless, online and non-adversarial**. A discrepancy first arrives as a gentle SMS/e-mail "nudge" inviting the taxpayer to check the AIS and, if needed, revise or update the return — no officer visit, no documents to carry, an opportunity to self-correct **before** any notice.
- **To the Department:** analytics let a small workforce cover a very large taxpayer base. Instead of randomly picking cases, the Department targets **verified, risk-ranked** discrepancies, freeing scarce assessment capacity for genuine high-risk cases and widening/deepening the tax base efficiently.

INTRAC and CMCPC — the two engines

Project Insight operationalised two dedicated centres, and knowing the division of labour between them is a common exam point: - **INTRAC — Income Tax Transaction Analysis Centre:** the **analytics** engine. It performs data integration, data-quality monitoring, data warehousing, master-data management, data analytics, web/text mining, alert generation, enterprise reporting and research support. In short, INTRAC turns raw data into **insight** (risk scores and alerts). - **CMCPC — Compliance Management Centralized Processing Centre:** the **outreach** engine. It runs centralised, campaign-based compliance management — **e-campaigns, e-verification, notices and reminders** — in a faceless, non-intrusive manner, acting on the alerts INTRAC generates.

Mnemonic: **INTRAC analyses, CMCPC contacts.**

How Insight fits alongside ITBA and TRACES/CPC

Insight is the **intelligence and risk-analytics layer**. It complements — and does not replace — the operational systems: - **ITBA** — the assessment / workflow system where officers act on cases. - **CPC-ITR (Bengaluru)** — processes returns and issues refunds. - **TRACES / CPC-TDS** — processes TDS/TCS statements and issues Form 26AS credits.

Insight draws data from all of these, adds third-party and foreign data, risk-scores it, and **pushes cases and information back to AOs through ITBA** for action. Insight supplies the intelligence; ITBA, CPC-ITR and TRACES carry out the operational processing and enforcement.

How officers use the Insight portal in practice — reports, monitoring and recovery support

For the field officer the Insight portal is not merely a repository of alerts; it is a working analytical tool through which routine management reports, monitoring returns and recovery leads are prepared. Access is role-based and jurisdiction-mapped (position/function code to jurisdiction, drawn from HRMS), so an officer sees the entities within the assigned charge. The functionalities most used in day-to-day work are:

- **Taxpayer Profile View** (*Insight → Profile → Taxpayer Profile View*) — a consolidated, aggregated view of a taxpayer's transactions, relationships and alerts drawn from ITR, TDS/TCS, SFT and other sources.
- **Business Intelligence (MIS)** — multi-dimensional reports organised under themes including **Tax Collection, Tax Base, ITR Information, Business Information, TDS Information, Litigation and Demand Management, and Faceless Assessment**, with drill-down, drill-up and drill-across facilities across jurisdictional hierarchies and time periods.
- **Insight Lens** — a query builder that lets an officer filter the database to a list of entities by parameters such as region, nature of taxpayer, turnover and financial ratios.
- **I-Search** — search across entities, accounts, contacts and addresses.

Use of the functionalities :

- **Preparing data on the highest tax payers of a charge/region.** Using the Tax Collection theme in Business Intelligence (and Insight Lens filtered to the jurisdiction), an officer can rank and list the **top taxpayers** of a charge, range or region. Such lists feed management reports, revenue-monitoring and review meetings, and help identify the entities that most influence the charge's collection.
- **Preparing data on advance-tax payers.** The same collection analytics allow the officer to compile the **advance-tax payers** of the charge and track instalment-wise payments across the year. This supports **advance-tax monitoring** — spotting taxpayers whose advance-tax payments have fallen relative to earlier years or relative to their known turnover/income, so that timely follow-up can protect the collection target.
- **Comparative analysis of an assessee's data across years.** Through the Taxpayer Profile View and the multi-year, drill-across reporting, an officer can compare a single assessee's **income, turnover, TDS, tax paid and reported transactions year on year**. A sharp fall in declared income against steady high-value transactions, or a dip in advance tax against a rising turnover, stands out and can be taken up for verification.
- **Identifying recovery-related possible assets of a defaulter.** Where a demand is outstanding, an officer (on invoking the appropriate access reason, such as **Recovery of Demand**) can use the Profile View to surface the defaulter's **financial footprint** — bank and deposit accounts, immovable property, securities and mutual-fund holdings, and other high-value transactions reported through SFT/AIS. These become leads for attachment or a garnishee notice (garnishee notice — see Chapter 10), aiding recovery under the Second Schedule.
- **Finding out collectible/recoverable demand.** The Litigation and Demand Management theme lets the officer view outstanding demand against a taxpayer or across the charge and separate the **collectible/recoverable** portion from demand that is stayed, disputed in appeal or otherwise not presently realisable. Read together with the asset information above, this helps focus recovery effort on demand that can actually be collected.

Because all of this rests on the same PAN-linked warehouse, the reports are only as good as the underlying data; the identity-resolution and data-quality safeguards described below are therefore essential to their reliability.

Data handling and the process flow of Insight

The value of Insight lies in the breadth of data it links to each PAN, the discipline with which it cleanses and secures that data, and the pipeline through which raw records become risk-ranked cases.

The data sources

Principal sources include: - **Statements of Financial Transactions (SFT)** under **section 285BA** r.w. **Rule 114E** — Form 61A (high-value transactions reported by banks, registrars, companies, etc.). - **TDS/TCS statements** (24Q/26Q/27Q/27EQ) processed at CPC-TDS (TRACES). - **ITR data**, and tax-payment data — advance tax / self-assessment challans (OLTAS) and refunds. - **Form 60/61** declarations (where PAN is not available) and **Form 61B** (FATCA/CRS foreign-account information). - **Foreign / exchange-of-information data** under **CRS** (OECD Common Reporting Standard) and **FATCA** (India–US IGA), and treaty exchange. - **Other third-party & open-source data** — e.g., GST turnover, registrar-of-property data.

The process and safeguards

- **Ingestion & integration:** data is collected from reporting entities and internal systems, then **cleansed, standardised and de-duplicated**.
- **Identity resolution to a single taxpayer view:** every record is linked to the correct **PAN/Aadhaar**, building one consolidated taxpayer profile (master-data management at INTRAC).
- **Data quality:** validation, standardisation and identity resolution reduce false matches (e.g., two people of the same name).
- **Masking, security & confidentiality:** sensitive data is **masked / access-controlled**; officers see information on a **need-to-know, role-based** basis with full **audit trails**. Access is governed by the confidentiality principles of **section 138** of the Income-tax Act.

Process flow — step by step

1. **Data acquisition** — SFT, TDS/TCS, foreign data, ITR and challan data flow into the warehouse.
2. **Processing & integration** — cleansing, de-duplication and linkage to PAN builds the taxpayer profile.
3. **Risk assessment / rule engine** — analytics and risk rules generate **risk scores** and **alerts** (potential non-filers, apparent under-reporting, high-value-transaction mismatches).
4. **Case selection** — high-risk cases are identified; some feed **CASS (Computer Assisted Scrutiny Selection)** and risk-based selection, others feed compliance campaigns.
5. **Dissemination to AOs** — verified information/cases are pushed to the **AO / range** through Insight and **ITBA** for action (scrutiny, verification, or reopening u/s 147/148 where warranted).
6. **Compliance management** — before any coercive action, **CMCPC** runs non-intrusive e-campaigns and e-verification, giving taxpayers the first chance to self-correct.

What third-party reporting (SFT) is — section 285BA / Rule 114E

A **Statement of Financial Transactions (SFT)** is a report that **specified persons** must file telling the Department about prescribed **high-value financial transactions** they have registered, recorded or maintained during the year. The legal obligation is in **section 285BA** of the Income-tax Act, 1961; the **details** — who must report, which transactions, and the monetary thresholds — are in **Rule 114E**. The statement is furnished in **Form 61A**.

Why third-party reporting matters

- **To the Department:** it supplies an **independent, corroborating stream** of information. If a person buys property worth ₹80 lakh but declares income of ₹3 lakh, the registrar's SFT surfaces the mismatch automatically, without any exploratory enquiry. SFT is the raw material of AIS and of e-verification.
- **To the taxpayer:** the same data is shown back in the **AIS and pre-filled return**, reducing errors and omissions, and giving a chance to reconcile or correct before scrutiny. Reporting is a duty of the **reporting entity**, not the taxpayer — the taxpayer benefits from the transparency.

Who reports and how — reporting entities, ITDREIN and due dates

- **Reporting entities/persons** include banks, post offices, co-operative banks, NBFCs, companies issuing shares/bonds/debentures, companies buying back shares, mutual funds, foreign-exchange dealers, sub-registrars of property, and any person liable to audit under s.44AB (for cash receipts > ₹2 lakh for sale of goods/services).
- They register on the **Reporting Portal** and obtain an **ITDREIN (Income Tax Department Reporting Entity Identification Number)**; a **Principal Officer / Designated Director** is registered.
- Statements are filed in the prescribed utility/format with a **digital signature**.
- **Form 61A (SFT)** is due **on or before 31 May** following the financial year; SFT for **listed securities and mutual-fund units** is filed **half-yearly**.

Illustrative SFT thresholds (Rule 114E)

Cash deposits/withdrawals in bank accounts (aggregate **₹50 lakh** current / **₹10 lakh** savings); cash payment for bank drafts / pre-paid instruments (**₹10 lakh**); time deposits (**₹10 lakh**); credit-card payments (**₹1 lakh** cash / **₹10 lakh** otherwise); purchase of bonds/debentures, shares, mutual-fund units, buy-back of shares, foreign currency (each **₹10 lakh**); **immovable property (₹30 lakh)**; and **cash receipt for sale of goods/services exceeding ₹2 lakh**. For threshold-based transactions, amounts across all accounts of the same nature are **aggregated**. Some categories reported through other channels (dividend, interest, capital gains) are captured **without a threshold**.

The reporting forms — 61A, 61 and 61B

Form	Purpose	Filed under
Form 61A	Statement of Financial Transactions (SFT) — high-value transactions	s.285BA r.w. Rule 114E
Form 61	Particulars of **Form 60** declarations received (transactions where PAN not quoted)	Rule 114D
Form 61B	Statement of **Reportable Accounts** under FATCA & CRS	Rule 114F–114H (Rule 114G)

- **Form 60** is the declaration a person files when they do not have a PAN; **Form 61** is the reporting entity's statement consolidating those Form 60 declarations (half-yearly).
- **FATCA** = the India–US Inter-Governmental Agreement (US persons); **CRS** = the OECD multilateral Common Reporting Standard (non-residents generally). Financial institutions report both in **Form 61B**.

What AIS (Annual Information Statement) is

The **Annual Information Statement (AIS)** is a **comprehensive, PAN-wise statement of a taxpayer's financial year** shown on the Compliance Portal (reachable from the e-filing site). It consolidates information across many categories — salary/TDS-TCS, interest, dividend, sale/purchase of securities and mutual funds, immovable-property transactions, foreign remittances, GST turnover and more. Crucially, for each piece of information AIS shows **two values**: the **reported value** (what the reporting entity reported) and the **modified value** (after the taxpayer's feedback is considered).

What TIS (Taxpayer Information Summary) is

The **Taxpayer Information Summary (TIS)** is the **category-wise, de-duplicated aggregate** derived from AIS. Where AIS is the detailed line-by-line ledger, **TIS is the clean summary** — one figure per category (e.g., total interest, total dividend). TIS is what the system uses to **pre-fill the ITR**, and it **updates dynamically** when the taxpayer's AIS feedback is accepted.

Why AIS/TIS matter

- **To the taxpayer:** AIS gives a **single complete view** of all financial activity linked to the PAN, so nothing is inadvertently omitted; TIS **pre-fills the return**, cutting effort and error; and the **feedback facility** lets a taxpayer flag wrong or duplicate entries before filing.
- **To the Department:** AIS is the **cross-verification tool** — it lets the system (and later the AO) compare declared income against third-party data, and it is the surface on which **e-verification mismatches** are shown and resolved.

AIS feedback options

For each entry the taxpayer can respond, e.g.: **Information is correct**; **Information is not fully correct**; **Income is not taxable / relates to other PAN or year**; **Duplicate / included in another information**; **Denied** (transaction did not happen). Accepted feedback flows into the **modified value** in AIS and the **accepted value** in TIS, which then drives pre-fill.

How AIS differs from Form 26AS

The distinction is frequently tested and is summarised in Chapters 05–06. For this chapter, the operative points are: Form 26AS is the tax-credit statement from which TDS credit is claimed, and its errors are corrected only when the deductor revises the TDS statement; AIS is the wider transaction statement carrying the taxpayer-feedback mechanism unique to the Compliance Portal, and its errors are corrected through feedback. Rule of thumb: 26AS to confirm tax credits; AIS to review all income; TIS to check the category totals to be declared.

What the e-Verification Scheme, 2021 is — section 135A

Section 135A of the Income-tax Act, 1961 empowers the Central Government to notify a scheme for the **faceless collection of information** (in relation to the information-gathering powers under **sections 133, 133B, 133C, 134 and 135**), to make the process efficient, transparent and accountable by **eliminating the interface** between the income-tax authority and the person, to the extent technologically feasible. Under this power the **e-Verification Scheme, 2021** was notified by CBDT on **13 December 2021 vide Notification No. 137/2021**.

Object: to **share and verify**, in a faceless and non-intrusive way, financial-transaction information that appears **unreported or under-reported** in a taxpayer's ITR — so the taxpayer can **voluntarily comply** before any scrutiny or reassessment.

The mismatch and "nudge" process — step by step

1. **Mismatch identified:** third-party information (SFT, TDS, foreign data) is risk-processed in Insight/CMCPC. Where it appears inconsistent with the ITR, an **information mismatch** is flagged and shown in the taxpayer's **AIS / Compliance Portal**.
2. **The nudge:** the taxpayer is prompted through an **e-campaign / "nudge"** (SMS / e-mail) to view the mismatch and respond. (CBDT describes this data-led outreach as the **NUDGE** approach — *Non-intrusive Usage of Data to Guide and Enable*.)
3. **Online response:** an **on-screen functionality on the Compliance Portal** lets the taxpayer **reconcile and submit a response online**; it is self-contained and **no documents need be uploaded**.
4. **Risk-based routing:** if the mismatch persists after initial e-verification, the information is run through the **CBDT risk-management strategy**. Low/no-risk items are **closed**; the rest are allocated (through an automated allocation system by the Pr.DGIT/DGIT-Systems) to the **Prescribed Authority** for verification.

5. **Voluntary correction:** where the taxpayer **agrees** with the under-reporting, the option to file an **Updated Return (ITR-U) under s.139(8A)** is offered to make good the shortfall — the softest possible resolution.
6. **Escalation only if needed:** if a satisfactory response is not received and the discrepancy persists, the **final verification report** is made available to the **Faceless/Jurisdictional AO** (if it relates to a pending scrutiny) or used for further action under the Act — e.g., scrutiny or reassessment.

Who administers it — the Prescribed Authority

The verification under the Scheme is carried out by the **Prescribed Authority** under procedures laid down by the **Director-General of Income-tax (Intelligence & Criminal Investigation) — DGIT (I&CI)**, with CBDT approval. CBDT has since issued operational guidance (e.g., **e-Verification Instruction No. 2 of 2024** for handling high-risk e-verification cases) and FAQs.

Why the e-Verification Scheme matters — soft-touch compliance

- **To the taxpayer:** it is a **pre-litigation, self-correction** opportunity — respond online, no personal appearance, no document upload, and a clean route (ITR-U) to fix genuine mistakes, avoiding penalty and prosecution exposure that scrutiny might bring.
- **To the Department:** it resolves large volumes of discrepancies **without opening formal proceedings**, reserving scrutiny/reassessment for the residue of genuinely non-compliant, high-risk cases — improving both **collections and taxpayer trust**.

The e-campaign / "nudge" in practice

Before any formal proceeding, the Department runs **electronic compliance campaigns** on the Compliance Portal, prompting taxpayers to verify their information and, where needed, **file or revise/update** returns. This "**trust taxpayers first / non-intrusive**" method has been used to resolve income and transaction mismatches for past assessment years and to prompt non-filers who nevertheless had high-value transactions. It embodies the philosophy that the **first response to a discrepancy is an invitation, not a notice**.

What SAKSHAM NUDGE is — CBDT's data-driven, non-intrusive nudge framework

SAKSHAM NUDGE is CBDT's formal, institutionalised framework for **non-intrusive, data-driven, taxpayer-friendly compliance**. **NUDGE** = *Non-intrusive Usage of Data to Guide and Enable* taxpayers — a strategic blend of behavioural economics, data analytics and risk identification that seeks to **inform, empower and facilitate** taxpayers into voluntary, accurate compliance in a collaborative, **non-adversarial** manner. Its two guiding principles are **"Trust First, Scrutinize Later"** and **"Turning Data into Revenue."** In effect, NUDGE is the philosophy behind the e-campaign / "nudge" already described under the e-Verification Scheme; **SAKSHAM** is the structured, seven-stage *strategy of implementation* that operationalises it end-to-end.

NUDGE is not a new data system — it **runs on the same rails** as the rest of this chapter: **Insight/INTRAC** for analytics and risk-scoring, **AIS/TIS and SFT/AEOI** as the information base, the **Compliance Portal / e-filing portal** for outreach (SMS, e-mail, pop-ups, portal alerts), and the **Updated Return u/s 139(8A)** as the standard self-correction route. Where the e-Verification Scheme, 2021 is the **statutory** faceless-verification mechanism, SAKSHAM NUDGE is the **campaign framework** that wraps around it — planning, targeting, messaging and evaluating behavioural-compliance campaigns.

The SAKSHAM seven-stage strategy

SAKSHAM (Hindi for "capable/empowered") is a **cyclical, continuous-learning** framework of seven interconnected stages; monitoring is not a terminal step but feeds back into any earlier stage. **AI and analytics are embedded at every stage. - SANKALAN (Collection & Compilation)** — build a reliable data ecosystem: collect, consolidate, validate and structure data from internal sources (ITR, TDS, SFT, AIS/TIS, Form 26AS) and external sources (AEOI/SEOI, public-domain and request-based data), with audit trails and data lineage. - **ANUSANDHAN (Research & Analytics)** — convert raw data into actionable intelligence: rule-based logic, statistical methods, risk scoring and machine-learning models to frame a **risk hypothesis**, cross-verify (e.g. AIS vs ITR, TDS vs declared income) and segment taxpayers (high-/moderate-risk, likely compliant, needs education). - **KRIYANVYAN (Action & Execution)** — *plan* the intervention: design behaviourally-informed NUDGE messages (social-norm framing, loss aversion, salience, simplification), pick channels, prepare taxpayer-centric templates and a campaign calendar, and vet content for legal correctness. - **SAMPARK (Communication)** — *execute*: deploy the approved multi-channel campaign (SMS, e-mail, portal notifications, pop-ups, outreach calls), monitor delivery/reach, handle queries and run reminder/escalation nudges. (Kriyanvyan plans; Sampark executes.) - **HASTAK (Handholding)** — reduce friction so the taxpayer can actually act: guided compliance journeys, clickable action links, helpdesks/chatbots/FAQs, trained support staff, and extra help for vulnerable segments (senior citizens, *divyang*, small businesses, digitally inexperienced). - **ADHIKAAR (Empowerment)** — rights-based enablement: make taxpayers aware of their statutory options and give a clear, non-intimidating route to **voluntarily correct** via updated/revised returns, presenting all legal routes with their tax/interest/fee consequences so the choice is informed and voluntary. - **MULYANKAN (Evaluation & Feedback)** — measure outcomes against KPIs (conversion rate, voluntary-filing uplift, tax recovered, risk reduction), study impact (e.g. RCT / difference-in-difference), document lessons and feed refinements back into future campaigns — closing the cyclical loop.

Mnemonic ordering: **Sankalan → Anusandhan → Kriyanvyan → Sampark → Hastak → Adhikaar → Mulyankan** (collect → analyse → plan → contact → handhold → empower → evaluate).

Why SAKSHAM NUDGE matters

- **To the taxpayer:** it is the **softest, pre-litigation touch** — a gentle SMS/e-mail/pop-up prompt (often at the time of filing) with step-by-step guidance and a clean route (ITR-U u/s 139(8A)) to self-correct, **before** any scrutiny, search or reassessment. It reduces friction and compliance cost, respects taxpayer autonomy ("Trust First"), and offers transparency about the data the Department holds.
- **To the Department:** it drives **large-scale voluntary compliance** using data the Department already has, resolving discrepancies in volume without intrusive enforcement, **widening and deepening the tax base**, and reserving scarce scrutiny/investigation capacity for genuinely high-risk residue — a scalable, replicable model of behavioural, technology-led governance.

Legal & procedural references

- **Section 135A**, Income-tax Act, 1961 — faceless collection of information / e-verification (basis of the e-Verification Scheme, 2021); operates in relation to ss.133, 133B, 133C, 134, 135.
- **e-Verification Scheme, 2021** — CBDT Notification No. **137/2021 dated 13.12.2021**; CBDT FAQs; e-Verification Instruction No. 2 of 2024.
- **Section 285BA** & **Rule 114E** — obligation to furnish SFT (Form 61A).
- **Rule 114B–114D** — Form 60 / Form 61 (declarations where PAN not quoted).
- **Rule 114F–114H (114G)** — Form 61B (FATCA/CRS reportable accounts).
- **Section 139(8A)** — Updated Return (ITR-U), the compliance route after e-verification.
- **Section 285BB / Rule 114-I** — Annual Information Statement / Form 26AS.
- **Section 138** — confidentiality principles governing access to taxpayer information.

Key Takeaways

- **Project Insight** is the Department's **Data Warehousing & Business Intelligence** platform enabling **data-driven, non-intrusive compliance**; objectives = promote voluntary compliance, deter non-compliance, ensure fair administration.

- Two engines: **INTRAC** analyses (analytics, risk scores, alerts); **CMCPC** contacts (centralised e-campaigns, e-verification). Insight feeds cases to AOs via **ITBA**.
- Three portals: **Insight portal** (officers), **Reporting Portal** (reporting entities file SFT, get **ITDREIN**), **Compliance Portal** (taxpayers — AIS, e-campaigns, responses).
- Officers use the Insight portal as a working tool — **Taxpayer Profile View**, **Business Intelligence/MIS** (themes including Tax Collection and Litigation and Demand Management), **Insight Lens** and **I-Search** — to prepare data on the **highest tax payers** and **advance-tax payers** of a charge/region, run **year-on-year comparative analysis** of an assessee, trace a defaulter's **assets for recovery**, and identify **collectible/recoverable demand**.
- **SFT** under **s.285BA r.w. Rule 114E** in **Form 61A**, due **31 May**; immovable-property threshold **₹30 lakh**, current-account cash **₹50 lakh**; third-party reporting supplies independent cross-verification data.
- **Form 61** = Form 60 declarations (Rule 114D); **Form 61B** = FATCA/CRS reportable accounts (Rule 114F–114H). FATCA = India–US IGA; CRS = OECD standard.
- **AIS** = wide transaction statement with **reported vs modified value** and **taxpayer feedback**; **TIS** = de-duplicated category summary that **pre-fills the ITR**.
- **AIS vs 26AS:** 26AS is the **tax-credit passbook** (TDS credit is claimed from **26AS**); AIS is the broader income/transaction view with feedback. Tax credit follows 26AS; AIS is completeness/cross-check.
- **e-Verification Scheme, 2021** notified under **s.135A** on **13 Dec 2021 (Notif. 137/2021)** — faceless verification of ITR/AIS mismatches; taxpayer responds **online, no documents uploaded**; remedy = **Updated Return u/s 139(8A)**.
- The **"nudge" / e-campaign** (NUDGE approach) is a **pre-litigation, soft-touch** prompt to self-correct — benefiting the taxpayer (self-correction) and the Department (volume resolution, scrutiny reserved for high-risk residue).
- The Scheme is administered by the **Prescribed Authority** under the **DGIT (I&CI)**; persistent, high-risk mismatches escalate to the Faceless/Jurisdictional AO for scrutiny or reassessment.
- **SAKSHAM NUDGE** is CBDT's institutionalised **non-intrusive, data-driven** compliance framework (**NUDGE = Non-intrusive Usage of Data to Guide and Enable**; principles: *"Trust First, Scrutinize Later"* and *"Turning Data into Revenue"*). It runs on Insight/AIS/AEOI data through **seven cyclical stages — Sankalan, Anusandhan, Kriyanvyan, Sampark, Hastak, Adhikaar, Mulyankan** — and powers campaigns (foreign assets via CRS/FATCA, s.80GGC, HRA, VDA, s.80G, F&B) with **ITR-U u/s 139(8A)** as the self-correction route.

Key terms & abbreviations

- **DW&BI** — Data Warehousing & Business Intelligence.
- **INTRAC** — Income Tax Transaction Analysis Centre (analytics).
- **CMCPC** — Compliance Management Centralized Processing Centre (outreach/e-campaigns).
- **SFT** — Statement of Financial Transactions (Form 61A).
- **ITDREIN** — Income Tax Department Reporting Entity Identification Number.
- **AIS / TIS** — Annual Information Statement / Taxpayer Information Summary.
- **NUDGE** — Non-intrusive Usage of Data to Guide and Enable (CBDT's data-led outreach).

- **SAKSHAM** — CBDT's seven-stage implementation strategy for NUDGE campaigns: **Sankalan** (collection), **Anusandhan** (research/analytics), **Kriyanvyan** (action/planning), **Sampark** (communication), **Hastak** (handholding), **Adhikaar** (empowerment), **Mulyankan** (evaluation).
- **AEOI / SEOI** — Automatic / Spontaneous Exchange of Information (CRS & FATCA foreign-account data feeding NUDGE campaigns).
- **FATCA** — Foreign Account Tax Compliance Act (US IGA); **CRS** — Common Reporting Standard (OECD). Both reported in Form 61B.
- **CASS** — Computer Assisted Scrutiny Selection.
- **ITR-U** — Updated Return under s.139(8A).
- **DGIT (I&CI)** — Directorate/Director-General of Income-tax (Intelligence & Criminal Investigation); Prescribed Authority under the Scheme.
- **Reporting entity** — bank/registrar/company etc. obliged to file SFT/Form 61/61B.

Part VI — HRMS & Information Security

16. HRMS in ITBA

Applicable to: ITO Paper-V, ITI Paper-IV, MS Paper-IV (all three cadres)

Syllabus reference: HRMS in ITBA — Role of HRMS in ITBA; the electronic Service Book and Employee ID; User roles and access levels; Role-Based Access Control (RBAC), least privilege and Segregation of Duties; HR compliance (CCS rules, APAR, vigilance).

Overview

The **Human Resource Management System (HRMS)** is the personnel-facing component of the **Income Tax Business Application (ITBA)**. Where the assessment, PAN, TDS and e-Verification modules manage *taxpayers*, HRMS manages the Department's own *personnel* — the complete service life-cycle of every officer and official, from joining and posting through leave, APAR, pay, training and deputation, to retirement and pension. HRMS is developed and owned by the **Directorate of Income Tax (Systems)**, with the **Human Resource Development (HRD) Directorate** and the **Pr. CCsIT / DGsIT** as administrative owners. Because it holds sensitive personal and service data of the entire workforce, HRMS is built on **Role-Based Access Control (RBAC)** and is tightly coupled with ITBA's single user-provisioning framework. This chapter first explains the underlying concepts — what HRMS is, what an Employee ID and Service Book are, what RBAC and least privilege mean, what APAR is, and how HR compliance ties to CCS rules and vigilance — and then sets out the HRMS functions, roles and controls in detail.

Foundational concepts — HRMS, the Employee ID and the Service Book

HRMS rests on two core records — the Employee ID and the electronic Service Book. Both are described below, ahead of the functions, roles and controls covered in the later sections.

What HRMS is

HRMS is a single, web-based application that digitises the **entire human-resource function** of the Income Tax Department. Instead of paper service books held in different offices, dozens of disconnected registers, and manual leave/APAR files, HRMS keeps **one electronic record per employee** and runs every HR process — posting, leave, appraisal, pay input, training, deputation, retirement — as a workflow on top of that record. It sits inside ITBA and shares ITBA's login, security and infrastructure.

Why an integrated HR system matters

The ITD employs tens of thousands of officers and officials spread across every State, organised in a deep field hierarchy. For an organisation of that size, an **integrated** HR system delivers what scattered paper cannot: - **Single source of truth.** One authoritative record means a transfer, promotion or increment is recorded once and is instantly visible to every authorised office — no divergent copies, no lost service books. - **Uniform rule enforcement.** Leave entitlements, APAR timelines and pension calculations are applied identically and automatically, reducing discretion and error. - **Speed and transparency.** An officer can apply for leave, file their property return or view their APAR online; approvals move electronically instead of by dak. - **Auditability.** Every action is logged, so seniority disputes, vigilance enquiries and audit objections can be settled from the system record. - **Feed to other systems.** HRMS is the *master* from which ITBA user accounts, pay inputs and pension orders are generated — one clean HR event drives many downstream actions.

In effect, HRMS converts HR administration from a manual, office-by-office activity into a **department-wide, rule-driven, data-backed** function.

The Employee ID

The **Employee ID** is the unique permanent number assigned to every ITD employee in HRMS. It stays with the individual for the whole career, irrespective of transfers or promotions. Critically, it is also the root of the person's ITBA identity: the ITBA login is created as **"U-Employee ID"** — i.e., the Employee ID prefixed to form the **ITBA User ID**.

The electronic Service Book

The **Service Book** is the official, career-long record of a government servant's service. Traditionally a physical booklet, in HRMS it becomes the **electronic Service Book (e-Service Book)** and holds: - bio-data, date of birth, home town, family and **nomination** details; - educational qualifications and technical qualifications; - date of joining, appointment order, confirmation, **seniority**; - **increment** history, pay fixation, and every pay/allowance change; - posting/transfer history and charge held; - leave account and leave events; - deputation, suspension, penalty, and other service "events" recorded under the rules; - retirement and pension particulars.

Why the Employee ID and Service Book matter

The Service Book is the **legal proof of service** — it decides seniority, eligibility for promotion, leave and pension entitlement, and settles disputes. An error or gap in it can cost an employee promotion or retirement benefits. Keeping it electronic in HRMS makes it tamper-evident (audit-trailed), always available to the competent authority, and directly usable to compute pension at retirement. The Employee ID ties this record unambiguously to one person and, through the U-Employee ID, ensures the *same* verified identity is used to access ITBA — a person cannot have HR data under one identity and system access under another.

Foundational concepts — RBAC, least privilege, APAR and HR compliance

The access-control and compliance concepts on which HRMS is built are set out below — RBAC and least privilege, the APAR, and how HR compliance ties to the CCS rules and vigilance.

What Role-Based Access Control (RBAC) is

Role-Based Access Control (RBAC) is a security model in which **permissions are attached to roles, and roles are assigned to users** — permissions are never granted directly to an individual. A "role" corresponds to a job or post (e.g., *DDO*, *Reporting Officer*, *CIT-Admin*, *HRMS Administrator*); it carries a defined bundle of things the holder may do and data they may see. When a person is placed in a post, they receive that post's role and, with it, exactly that bundle — no more. This is the model formalised by NIST, which describes RBAC in levels from **flat** (simple role assignment) through **hierarchical** (senior roles inherit permissions of junior ones) to **constrained** RBAC (adds separation-of-duty rules).

Least privilege — what it is and why it matters

The **principle of least privilege** means a user is given **no more privilege than is necessary to perform their current job — and nothing more**. You identify the job, determine the minimum set of permissions it needs, and confine the user to exactly that set.

Why it matters: - **Security / containment of impact.** If an account is misused or compromised, the damage is confined to that one role's narrow scope — an AO's compromised login cannot reach another charge's establishment data. - **Confidentiality of sensitive HR data.** Service records, APARs and property returns are sensitive personal information; least privilege ensures only those with a genuine functional need can see them, and even then only the records within their charge. - **Segregation of Duties (SoD) / fraud deterrence.** By splitting conflicting powers across different roles, no single person can both initiate and approve a sensitive action, closing off single-point manipulation and fraud. - **Accountability.** Because access maps to a defined role and every action is logged, responsibility for any change is unambiguous.

RBAC + least privilege together answer the core HR-data question — *who may do what, to whose record* — in a way that is uniform, enforceable and auditable across the whole Department.

What APAR is — and why it matters

The **Annual Performance Appraisal Report (APAR)** — earlier called the **Confidential Report / Performance Appraisal Report (PAR)** — is the yearly written assessment of an officer's performance, conduct and potential. It moves through a defined chain: the officer records a **self-appraisal**, the **Reporting Officer** grades and comments, the **Reviewing Officer** reviews, and the **Accepting Authority** accepts (with a numerical grading and a pen-picture). In HRMS the APAR is filed and routed **online**, and legacy paper APARs are stored as **scanned APARs**.

The APAR is the single most consequential document for an officer's career: it governs **promotions, empanelment, deputation selections and postings**. Grades below a benchmark, or adverse remarks, can stall a career — hence the rule that **adverse entries must be communicated** to the officer, who may **represent** against them. Because so much rides on it, the APAR process is time-bound and access-controlled: only the officers in the reporting chain may view or act on a given APAR, and the workflow enforces the sequence and the DoPT calendar.

HR compliance, CCS rules and vigilance

Government service is governed by a codified rule-book — chiefly the **Central Civil Services (CCS) rules** — covering conduct, leave, discipline, appeal and pension. HRMS is the **digital instrument** through which these rules are applied to ITD personnel: entitlements, filings, timelines and disciplinary outcomes are all recorded and enforced in the system, and the record interfaces with the **vigilance / disciplinary** machinery.

Compliance is not optional book-keeping — it protects both the employee (correct entitlements, fair process) and the Department (integrity, defensibility). A disciplinary penalty, a sealed-cover instruction, or a pending vigilance case has direct effects on increments, promotion and pension; recording them accurately against the service record, with an audit trail, is what makes those effects lawful and defensible. Conversely, misuse of HRMS access (unauthorised viewing or disclosure of another's records) is itself a **conduct violation**. Thus HR compliance, CCS rules and vigilance are woven into HRMS rather than sitting outside it.

Role of HRMS in ITBA — the principal functions

HRMS is the **single authoritative repository of service records** and the engine for HR processes. Its principal function areas:

Function area	What HRMS does
Service Book / Employee master	Electronic Service Book — bio-data, family & nomination, education, seniority, increment history, all service "events".
Postings, transfers, hierarchy	Records office, charge (RCC/Region–CCIT–CIT–Range–AO), designation and posting history; transfers / AGTs (Annual General Transfers) update the mapping.
Leave management	Leave account (EL / HPL / CL / Commuted / EOL / CCL etc.), application–sanction workflow, balances per CCS (Leave) Rules.
APAR / PAR	Online APAR — Basic Info, Self-appraisal, reporting/reviewing/accepting workflow, and scanned legacy APARs.
Pay & allowances	Feeds pay, increments and allowances; works with the **Data Collection Portal (DCP)** and DDO functions for payroll inputs.
Training	**Training Management Module** — course creation, nomination/enrolment, NADT/RTI records, feedback.
Deputation	Deputation in/out, lien, pension contribution and leave during deputation.
Self-service / IPR	**Employee Self Service** including **Immovable Property Return (IPR)**; **Officer Self Service** for Group-A/B.
Retirement & pension	Retirement processing and **e-PPO** generation — pensioner data and e-signed PPO flow through HRMS.
ID Card & misc.	ID Card Management Module, Recruitment module, handover/takeover.

The subtopics below expand several of these.

The e-Service Book and employee master

This is the core record of HRMS. Every other module reads from or writes to it. Because it is the *master*, correctness here is paramount — an increment or seniority error propagates into promotion eligibility and pension.

Postings, transfers and the charge hierarchy

HRMS maps each employee to an **office and charge** in the field hierarchy (RCC → Region → CCIT → CIT → Range → AO/Ward). **Annual General Transfers (AGT)** and interim transfers are recorded here; this mapping is what drives *data visibility* under RBAC — an officer sees the establishment of the charge they currently hold.

Leave management

The leave module holds each employee's **leave account** and runs the apply → sanction workflow, automatically maintaining balances (EL, HPL, CL, Commuted Leave, EOL, Child Care Leave, etc.) in line with the **CCS (Leave) Rules, 1972**. The applicant and the sanctioning authority are necessarily different roles.

APAR / PAR module

Implements the online APAR workflow (see the concept explainer above), plus storage of **scanned** older APARs. The workflow proceeds in five stages: 1. **Basic Info**; 2. **Self-appraisal** by the officer; 3. **Reporting** by the Reporting Officer; 4. **Reviewing** by the Reviewing Officer; and 5. **Accepting** by the Accepting Authority.

Note the distinct access requirement: opening the APAR link requires **User ID + ITBA password + a separate HRMS password + RSA token**, reflecting the sensitivity of appraisal data.

Pay, allowances and the Data Collection Portal (DCP)

Payroll inputs (pay, increments, allowances, deductions) are captured through **DDO functions** and the **Data Collection Portal (DCP)**, which feed the salary process. There are DCP user manuals for both the **DDO** and the **employee**.

Training Management Module

Handles the training cycle — **course creation, nomination and enrolment, records of NADT/RTI training, and feedback**. It is also a clean illustration of role-based access in practice (see below).

Deputation

Records deputation in/out, **lien**, pension contribution and leave during the deputation period — events that must reconcile back to the parent-cadre service book.

Employee Self Service, Officer Self Service and IPR

Through **Self Service**, an employee views their own record and files returns — most importantly the **Immovable Property Return (IPR)** required under the conduct rules. **Officer Self Service** covers Group-A/B officers.

Retirement and e-PPO

At superannuation, HRMS drives retirement processing and generates the **e-PPO (electronic Pension Payment Order)** — pensioner data (XML) plus an **e-signed PPO PDF** — which the pensioner can access in **My Services**. This closes the service life-cycle inside the same system that opened it.

ID Card, Recruitment and handover/takeover

Ancillary modules — **ID Card Management**, **Recruitment**, and **handover/takeover** on relief — round out the HR functions.

HRMS as the source of ITBA user provisioning

A defining feature is that **HRMS drives ITBA identity**. The **Employee ID** becomes the **ITBA User ID (U-Employee ID)**. An HR event in HRMS is the *trigger* that creates, modifies or deactivates the corresponding ITBA login and role: - **On joining** → the account and initial role are created. - **On transfer / promotion** → the old role is withdrawn and the new post's role is granted. - **On relief / retirement** → the account/role is deactivated.

Thus HRMS is not a stand-alone system; it is the **system of record for "who works for the Department and in what capacity,"** and all ITBA access flows from it. This is exactly why HR-data accuracy has security consequences well beyond HR.

Access channels and authentication

Select modules (HRMS, Employee Self Service including IPR, APAR, Officer Self Service) are made available **over the internet using SSL VPN** so officers can work from anywhere. **All Group-A and Group-B officers** access these using **ITBA User ID (U-Employee ID) + ITBA password + RSA token** at the VPN portal. Some screens need an **additional HRMS password** (e.g., APAR). **Digital Signature Certificates (DSC)** are used to e-sign HR letters, orders, APARs and pension documents.

User roles and access levels

A user's **functions and data visibility are decided by the role attached to the post they hold, not by the individual**. Broadly:

Role / level	Typical functions & data scope
Employee (Self Service)	View own service book, apply for leave, file IPR, self-appraisal, payslip, training history, ePPO. Sees **only own data**.
DDO / Office (admin staff)	Pay/allowance inputs, leave data entry, DCP entries for the office. Scope limited to **own office / DDO unit**.
AO / ITO / Reporting Officer	Initiates/records APAR for subordinates; sanctions leave within delegated powers; views service data of reporting staff.
Range Head (Addl./Jt. CIT) / Reviewing Officer	Reviews APARs; forwards HR proposals; visibility over the **Range's** employees.
PCIT / CIT (Admin) / Accepting Authority	Accepts APARs; sanctions transfers/leave/deputation within powers; visibility over the **charge's** establishment.
HRD / Pr.CCIT (CCA) / Cadre Controlling Authority	Cadre management, promotions, AGT, vigilance/disciplinary linkage; visibility over the **Region/cadre**.
HRMS Administrator / Workflow Admin (DIT-Systems / Regional)	Role assignment, user creation, ID-Card admin, technical configuration; **no business approval powers** — administrative only.

The same screen behaves differently for different officers

Because permissions ride on the role, one physical screen shows a Range Head a worklist and approval buttons that an AO does not see, while an employee sees only their own record. **Hierarchy in HRMS mirrors the field hierarchy**, so data visibility cascades **downward** (a superior sees subordinates' records relevant to their function) and **never upward or sideways** beyond the sanctioned scope.

Illustration — Training Management access

The Training module shows role-tiering concretely: the **Employee Self-Service (ESS)** part does **not** require an RSA token, but the **Admin** functionalities of the same module **do** require the RSA token. Same module, different roles, different security gates.

Role-Based Access Control (RBAC) as applied in HRMS

RBAC is the security model on which HRMS (and ITBA generally) is built — permissions to roles, roles to users, never permissions to individuals. The applied principles are set out below.

Least privilege in practice

A user gets only the minimum access needed for their current post — an AO cannot open another charge's establishment data; a DDO cannot edit APARs; an employee can see only their own record.

Access follows the chair, not the person

When an officer is transferred or promoted (itself an HR event in HRMS), the **old role is withdrawn and the new post's role is granted**. On relief/retirement the login is deactivated. This prevents an officer from carrying away access to a charge they have left — a common weakness in person-based permission schemes.

Segregation of Duties (SoD)

Conflicting functions are split so that no single person both initiates and approves: - the officer who **records** an APAR (Reporting) is different from the one who **reviews** and the one who **accepts**; - **leave applicant ≠ sanctioning authority**; - the **HRMS administrator** who creates users does **not** exercise business approvals.

This is the classic anti-fraud control: because sensitive transactions need two or more mutually exclusive roles to complete, collusion would be required to manipulate the record — a far higher barrier than manipulation by a single individual acting alone.

Maker–checker workflow

HR actions move through an **initiator → approver** chain with electronic sign-off, often using **DSC**, so every substantive change carries a second, independent authorisation.

Audit trail and non-repudiation

Every login, view, data change and approval is **logged with user ID, role, date-time and action**. This gives **non-repudiation** (a signed/logged action cannot credibly be denied) and an evidence trail for vigilance and audit. **RSA token + SSL VPN** secure remote access.

Multi-factor authentication binds the role to the real officer

Identity is multi-factored — **User ID + password(s) + RSA OTP token**, with **DSC** for signing — so the role's powers are reliably tied to the actual, verified individual, and the audit trail is meaningful.

HR compliance and the CCS rule-book

HRMS is the digital instrument for enforcing the Government's HR rules on ITD personnel. The principal rule-sets are set out below.

CCS (Conduct) Rules, 1964

Govern integrity and conduct — **IPR filing** (captured in HRMS Self-Service), restrictions on private trade, acceptance of gifts, and general behaviour. HRMS holds the IPR and conduct-related records. Misuse of HRMS access is itself a conduct violation under these rules.

CCS (Leave) Rules, 1972

Define leave entitlements, accumulation, encashment, Child Care Leave and EOL — all operationalised through the HRMS leave module and its running balances.

CCS (CCA) Rules, 1965 — Classification, Control & Appeal

The disciplinary framework — **minor and major penalties, suspension, charge-sheets, appeals** — and the vigilance/disciplinary interface. Penalty orders and their effect on increments and promotion are reflected against the service record.

CCS (Pension) Rules

Retirement and pension processing — **qualifying service, commutation, e-PPO** — handled in the pension/retirement workflow at superannuation.

APAR timelines (DoPT calendar)

The online APAR follows the prescribed calendar — self-appraisal by the employee, report by the Reporting Officer, review by the Reviewing Officer, and acceptance — with the completed APAR ordinarily to be **finalised by 31 December of the calendar year in which the reporting year ends (e.g., the APAR for FY 2023-24 by 31.12.2024). Adverse remarks must be communicated** and the officer allowed to represent. HRMS enforces these stages and dates.

Data privacy of employee records

Service data is **sensitive personal information**; RBAC + least privilege + audit trail restrict access strictly to authorised roles, and unauthorised viewing or disclosure is a conduct violation. Departmental data handling aligns with **IT Act, 2000** safeguards and Government data-security instructions; the DPDP Act, 2023 is the emerging privacy framework but is not yet fully operational (position as on FY 2024-25).

Vigilance and disciplinary interface

Vigilance status, **sealed-cover** procedure, and pending disciplinary proceedings interface with HR decisions — **promotion, posting, pension** — and the HRMS audit trail supports such proceedings by evidencing who did what and when.

Legal & procedural references

- **CCS (Conduct) Rules, 1964; CCS (Leave) Rules, 1972; CCS (CCA) Rules, 1965; CCS (Pension) Rules** — governing service conduct, leave, discipline and pension.
- **DoPT APAR guidelines** — online APAR stages and timelines (finalisation generally by 31 December of the following year); communication of adverse remarks.
- **ITBA-HRMS / ITBA-Internet Instructions issued by DIT(S) / DGIT(Systems)** (e.g., F.No. DIT(S)-3/HRMS series) — module roll-outs (HRMS, Training Management, DSC under ITBA/HRMS, Data Collection Portal) and internet/SSL-VPN access with RSA token.
- **IT Act, 2000 / DPDP Act, 2023** — data-protection backdrop for employee personal data (DPDP Act not yet fully in force).

Key Takeaways

- HRMS is the **ITBA module for the Department's own employees** — the electronic Service Book and all HR processes — distinct from taxpayer-facing modules; owned by **DIT(Systems) / HRD**.
- The **Employee ID** is the permanent unique key; it becomes the **ITBA User ID (U-Employee ID)**, so HRMS is the **source of ITBA user provisioning** — HR events create, modify or deactivate ITBA access.
- The **e-Service Book** is the legal proof of service (seniority, increments, pension); accuracy here drives promotions and retirement benefits.
- **RBAC** = permissions attach to **roles**, roles to **users**; access **follows the post, not the person** (old role withdrawn, new role granted on transfer/promotion; deactivated on retirement).
- **Least privilege** limits each user to the minimum access their post needs — bounding damage, protecting sensitive data, and enabling accountability.
- **Segregation of Duties** splits conflicting powers (APAR Reporting ≠ Reviewing ≠ Accepting; applicant ≠ sanctioner; admin ≠ business approver); the **audit trail** gives non-repudiation.
- Remote access uses **SSL VPN + RSA token** (extra **HRMS password** for APAR); HR documents are e-signed with **DSC**; Training ESS needs no RSA token but its Admin functions do.
- **APAR** stages: **Basic Info → Self-appraisal → Reporting → Reviewing → Accepting**; DoPT calendar (finalise ~**31 December** of the following year); adverse remarks must be communicated.
- Compliance backbone: **CCS Conduct / Leave / CCA / Pension Rules** + **DoPT APAR** timelines; vigilance/disciplinary actions (sealed-cover) interface with promotion, posting and pension.
- Key modules: **Service Book, Leave, APAR, Training Management, Pension/e-PPO, IPR (Self-Service), ID Card, Recruitment, DCP/DDO**.

Key terms & abbreviations

- **HRMS** — Human Resource Management System
- **ITBA** — Income Tax Business Application
- **RBAC** — Role-Based Access Control; **SoD** — Segregation of Duties
- **APAR / PAR** — Annual Performance Appraisal Report / Performance Appraisal Report
- **IPR** — Immovable Property Return
- **DCP** — Data Collection Portal; **DDO** — Drawing & Disbursing Officer

- **DSC** — Digital Signature Certificate; **SSL VPN** — Secure remote-access channel; **RSA token** — one-time-password device
- **e-PPO** — electronic Pension Payment Order
- **CCS (CCA) Rules — Central Civil Services (Classification, Control & Appeal) Rules, 1965; CCS also prefixes the Conduct Rules, 1964, the Leave Rules, 1972 and the Pension Rules. CCA (administrative usage) — Cadre Controlling Authority.**
- **HRD** — Human Resource Development (Directorate); **AGT** — Annual General Transfer
- **ESS** — Employee Self Service; **NADT** — National Academy of Direct Taxes; **RTI** — Regional Training Institute
- **DoPT** — Department of Personnel & Training; **DPDP Act** — Digital Personal Data Protection Act, 2023
- **DIT(S) / DGIT(Systems)** — Directorate / Directorate-General of Income Tax (Systems)

17. ITD Information Security Policy, 2020

Applicable to: ITO Paper-V and MS Paper-IV. (The syllabus lists the *ITD Information Security Policy, 2020* for the Income Tax Officer and Ministerial Staff papers.)

Syllabus reference: "ITD Information Security policy 2020."

Overview

The **ITD Information Security Policy, 2020 (ISP-2020)** is the Income Tax Department's apex internal security policy, issued by the CBDT (Foreign Tax & Tax Research Division) and itself marked **"Restricted."** It is a high-level "living document" framed on the lines of the **ISO/IEC 27001** family of controls and read **in conjunction with the earlier CISO Instructions, MHA information-security guidelines, CERT-In guidelines and the IT Act, 2000**. Its purpose is to protect the **confidentiality, integrity and availability (the "CIA triad")** of the Department's data — chiefly the sensitive financial and personal information of taxpayers held in systems such as **ITBA, Insight, TRACES, CPC and the e-filing portal**. The policy lays down *what* must be protected and *by whom*; it is then operationalised through a series of **CISO Instructions** (2022 and 2023) that spell out detailed controls, role-by-role action points, templates, checklists and audit procedures. This chapter follows the clauses of ISP-2020 and then summarises each of those CISO Instructions in turn.

Information security and the CIA triad — the core concepts

What is "information security"?

Information security is the protection of information and information systems from unauthorised access, use, disclosure, disruption, modification or destruction. It matters because the ITD holds one of the largest repositories of citizens' financial data in the country: PAN details, returns, bank information, foreign-asset data received under tax treaties, search/survey material and investigation records. A leak, tampering or outage in this data can cause identity theft, fraud, extortion, loss of public confidence, breach of India's international treaty obligations, and even damage to national interest. Information security is therefore not solely a matter for the IT function — under ISP-2020 **every officer and official who handles departmental data is personally responsible** for protecting it.

The CIA triad — what it is and why it matters

ISP-2020 (and every CISO Instruction) is built around three properties that must always be preserved:

- **Confidentiality** — information is disclosed only to authorised persons on a **need-to-know** basis. Example: a taxpayer's return should be visible only to the officers handling that case, not to the whole office.
- **Integrity** — information stays **accurate and complete** and is not altered or corrupted without authorisation. Example: a demand figure or an assessment order must not be silently modified.
- **Availability** — information and systems are **accessible to authorised users when required**, supported by backup, redundancy and business-continuity controls. Example: the assessment system must be up when an order is time-barring.

The Asset Management instruction operationalises this by rating each asset's **C, I and A** on a **scale of 1–3** (1 = negligible impact, 3 = severe impact); the asset's overall **criticality = max(C, I, A)**, giving a High/Medium/Low rating that decides how strongly it must be protected. Why it matters: this enables the Department to concentrate its limited protective resources on the assets whose compromise would cause the greatest harm.

Objective, scope and structure of ISP-2020

- **Objective (Clause 1.2):** to address and manage internal and external information-security risks and to protect the confidentiality, integrity and availability of data. It is a guiding reference from which individual offices develop detailed procedures.
- **Scope and applicability (Clause 1.3):** applies to **all offices under the Pr. CCsIT (CCA) in every region and all attached Directorates of CBDT**, to **all information assets** wherever hosted, and to **all employees, contractors, third-party staff and partners** who access ITD information or processing facilities.
- **Exception management (Clause 1.4):** every exception to the policy must be approved by the **CISO**.
- **A "living document" (Clause 1.2.3):** the CISO distributes and periodically reviews the policy so it keeps pace with new threats.

Data / information classification — what it is and why it matters

Before you can protect information you must know **how sensitive it is**. ISP-2020 (Clause 5.3) adopts the **Government of India classification scheme** — the same five levels used across the Union Government — rather than a generic "public/internal" scheme:

Class	Meaning	Handling (per Asset Management instruction)
Top Secret	Disclosure could cause *exceptionally grave* damage to national security/interest; the nation's closest secrets, used "with great reserve"	Label on footer, Document Control Table and removable media; restricted to designated high-level management; stored/transferred **encrypted** (SSL/PPTP/IPSEC); access logged
Secret	Disclosure could cause *serious* damage or serious embarrassment; the highest classification normally used	Labelled; strong encryption within and outside the network; hard copy in secure areas with access logged
Confidential	Disclosure could damage/prejudice the organisation; **most information, on proper analysis, is classified no higher than this**	Encrypted transmission; restricted-access storage; **must not be forwarded to personal e-mail** (Gmail/Hotmail); clear-desk
Restricted	Meant for **official use only**; not to be published/communicated except for an official purpose	Exchanged only with ITD/MSP/authorised stakeholders on official e-mail; access only after owner's approval
Unclassified	Needs no protection against disclosure (e.g. public website releases)	No labelling/security requirement

Why it matters: classification drives **every downstream control** — labelling, encryption, who may see it, how it is stored, and how it must be destroyed. ISP-2020 requires information to be **labelled** (classification in the footer of every page and on media labels) and handled commensurate with its class, with defined **retention, archival and secure-destruction** procedures.

Governance hierarchy — the information-security organisation (Section 2)

ISP-2020 builds a multi-tier governance pyramid (Clause 2). The apex roles are filled **ex-officio**, so responsibility attaches to the post, not the person.

Body / Officer	Clause	Who holds it	Core role
Information Security Committee (ISC)	2.1	Chaired by **Member (I/c FT&TR), CBDT**	Apex body; ratifies the ISP, oversees implementation/review, initiates security reviews, oversees disciplinary action for breaches
CISO, CBDT	2.2	**Commissioner (Coordination & Systems), CBDT**	Focal point for all security issues; establishes, operates, monitors and improves security; approves/maintains/communicates the ISP; approves all exceptions; reports to the ISC
LISC (Local Information Security Committee)	2.3	Set up in every Cadre-Controlling Pr.CCIT	Ensures regional compliance; initiates regional reviews; monthly reports to CISO
LISO (Local Information Security Officer)	2.4	**Commissioner (Admin)** of the region	Regional focal point for security
HoDs (Pr.CIT/Pr.DIT/CIT/DIT/ADG)	2.5	Heads of office	Communicate/implement policy; monitor staff; report incidents
BISO (Building Information Security Officer)	2.6	Officer **not below CIT rank** stationed in the building (nominated by LISO)	Physical and environmental security of the building; first responder for incidents
SISO (Systems Information Security Officer)	2.7	**ADG (Systems)(HQ)**	Focal point for the Directorate of Systems; tracks vulnerabilities/threats
PISO (Project Information Security Officer)	2.8	Addl./Jt./Dy. Director (Systems) per project/module	Project/module-level ISMS compliance
Commissioner (Audit)	2.9	CIT(Audit)	Conducts information-security audits of compliance

Why the hierarchy matters: it fixes **accountability at every level** — a policy is only as good as the named officer answerable for it. There are two distinct incident streams:

- **physical, HR and asset** incidents are escalated upward through the BISO, then the LISO, then the CISO; and
- **cyber** incidents are escalated to **AD/DD/JD (Systems)** in the Pr.CCIT(CCA) office.

Acceptable Use — passwords, communications and devices

The Acceptable Use rules translate the CIA triad into day-to-day conduct at the workstation. They cover authentication, the channels by which information moves, and the devices that can carry it out of the building.

Passwords

- All passwords (user and administrator) are **confidential and must never be shared, posted or divulged** (Clause 6.4).
- Initial passwords must be **force-changed at first logon**; passwords must be strong and non-guessable.
- **Two-factor authentication is mandatory for all critical systems** (Clause 6.4.4), and for tele-working/remote access (Clause 8.7.2).
- **Inactive accounts (no use for 45 days) are automatically disabled** (Clause 6.2.6).

Why it matters: a shared or weak password defeats every other control, because misuse then appears to come from a legitimate user.

E-mail, internet and messaging

- **E-mail (Clauses 8.8 and 8.10):** attachments must be anti-virus and content-scanned; **non-government e-mail (Gmail, Yahoo, Rediff, Hotmail) must NOT be used for classified information**, and Confidential e-mails must not be forwarded to personal accounts.
- **Internet (Clause 8.12):** no hacking, phishing or downloading/transmitting obscene material (referencing the **IT Act 2000 / IT (Amendment) Act 2008**); server logs are proof of misuse; each internet PC has a named custodian; proxy-avoidance tools and unauthorised instant messaging are barred. Internet/policy violations “shall lead to disciplinary action.”
- **Wi-Fi (Clause 8.13)** and network access (8.2) are controlled and monitored.

Removable media, mobile devices and BYOD

- **Removable media / USB (Clause 8.14):** USB ports on machines handling sensitive data are **blocked by default**; enabling them needs competent-authority approval and a service request; all media must be **scanned for malware** and serially numbered/labelled; execution of software directly from USB is prohibited.
- **Mobile devices & tele-working (Clause 8.7):** laptops/mobiles holding internal/confidential data require **hard-disk encryption**; remote access needs two-factor authentication; remote users must comply with the ISP before connecting.
- **Portable devices** must be password-protected with auto-lockout, and **defective storage media (e.g. hard disks) must never be handed to a vendor** — the faulty media is retained by the Department and made non-recoverable.

Why it matters: a single unencrypted pen-drive or laptop is the most common route for a large data leak, so the policy tightly controls anything that can carry data out of the building.

Access control and least privilege (Section 6) — the concept

Access follows the twin principles of **least privilege** (a user gets only the rights their job needs) and **need-to-know** (a user sees only the data their task requires). ISP-2020 gives effect to this through:

- a **formal registration/de-registration process** with documented approval (Clause 6.2), and prompt removal of access on transfer/exit;
- **privilege management** (Clause 6.3) that limits and monitors root/administrator accounts;
- **periodic review of access rights** (Clause 6.5); and
- **operating-system access controls** (Clause 6.7) — including **automatic screen time-out and clear after 5 minutes** of inactivity (6.7.7).

Why it matters: over-broad access is the greatest single insider-threat risk; least privilege limits how much damage any one compromised or malicious account can do.

Physical and environmental security (Section 11)

- Premises are divided into five **zones**, each with its own access controls, ranging from the least to the most restricted:

1. Public;
2. Reception;
3. Operations;
4. Security; and
5. High Security.

- Areas with critical IT equipment or **sensitive information (e.g. foreign-jurisdiction or investigation material) are High Security Zones** (Clause 11.1).
- **Server rooms / data centres** use **biometric access control** (Clause 11.1.3), restricted to authorised technical staff, with all openings **monitored round-the-clock by CCTV** (11.2.11).
- **Visitor controls (Clause 11.2):** identity check, frisking/bag check, confirmation from the visited officer, a visitor register (name, address, whom to meet, purpose, device declaration, in/out time), **no tailgating**, ID badges always worn, tight off-hours control.
- **External/environmental hazards (Clause 11.4):** firefighting equipment, fire and earthquake evacuation drills, flood/drainage protection, emergency lighting, UPS/alternate power.
- **Clear-desk / clear-screen (Clause 11.6):** documents locked in cabinets when away from the desk; screens locked; no "shoulder-surfing" of Confidential/Secret/Top-Secret information.
- **Secure disposal (Clause 11.14):** data destroyed before disposal by **physical destruction, three-pass digital wiping, or degaussing**.

Operations, backup and business continuity (Sections 7 & 14)

- **Backup (7):** all software, data, configurations and logs are backed up at a documented frequency; backups kept in **fire-rated containers**, with **both onsite and offsite copies in a fire-proof safe**; a backup register is maintained; **backups stay under departmental (not vendor) control**; restoration is tested.
- **Business continuity (14):** a Business Continuity Plan (BCP) with disaster-recovery procedures, tested **bi-annually**, plus redundancy to meet availability needs.

Incident reporting and response (Section 13) — what it is and why it matters

An **information-security incident** is any event that compromises (or threatens) the **CIA** of information/systems — including weaknesses, malfunctions and policy violations. Under Clause 13:

- Every employee/contractor must **report suspected weaknesses and incidents promptly** to BISO/LISO (Clause 13.1).
- Incidents are **logged, assessed, classified and escalated** per the Incident Management framework; management responsibilities and procedures ensure a "quick, effective and orderly response" (Clause 13.3).
- Relevant **authorities and CERT-In** are contacted where needed (Clause 13.2).
- **Evidence is collected and preserved** for possible legal action (Clause 13.4).
- A **breach of information received from foreign authorities under tax treaties** triggers a special protocol under **ISC supervision**.

Why it matters: fast, honest reporting limits damage and preserves evidence; hiding an incident usually makes it far worse and is itself a policy violation.

Third-party / vendor security (Sections 9 & 10)

Suppliers' security obligations are built into contracts/SLAs; **NDAs/confidentiality agreements** are signed by vendors, contractors and sub-contractors; subcontracting needs prior departmental permission; **vendor audits are conducted at least annually**; and backup/authorisation systems remain under departmental control.

The CISO Instructions — how ISP-2020 is put into practice

ISP-2020 is a framework; the **CISO Instructions** turn it into concrete duties, templates and checklists. The instructions below (all issued by the CISO, CBDT) are the current operational layer and are examinable alongside the parent policy.

CISO Instruction No. 1/2022 — Human Resource Security (21-01-2022)

Focuses on protecting information across the **employee lifecycle** — before, during and after employment. Its mandate:

- **Job descriptions** must document security roles/responsibilities; **background/verification checks** are mandatory for all personnel (including temporary and contract staff) in sensitive roles.
- **Terms & conditions** of employment must state security responsibilities; all employees, contractors and third-party users must sign **confidentiality/Non-Disclosure Agreements (NDAs)**.
- **Management responsibility:** PCsIT/PDsIT/CsIT/ADsG monitor staff conduct and its impact on security; the **Commissioner (Admn. & TPS) is the LISO** and regional focal point.
- **Information-security training and awareness** must be provided to all users, with periodic assessments.
- A **formal disciplinary process** (for employees) and **penal process** (for contractors/third parties) must exist for violations.
- On **termination/transfer**: orderly hand-over, **return of all assets**, and **immediate removal of physical and logical access rights**.
- Enclosures include HR-security procedures, guidelines, a **Confidentiality Agreement template**, a training-attendance template and an HR-security checklist.

CISO Instruction No. 2/2022 — Asset Management (21-01-2022)

Ensures adequate protection for ITD **assets, information and information-processing facilities** across their lifecycle. Its mandate:

- Maintain an **Information Asset Inventory** (with ID, description, location, **owner**, custodian, business value, classification and validity), covering information, software and hardware assets.
- **Classify** every asset (Top Secret → Unclassified) and rate its **C/I/A on a 1–3 scale**, deriving an **Asset Criticality = max(C,I,A)** (High/Medium/Low).
- Define **Acceptable Use** of assets (official/operational purposes only) and **media handling** — protection from fire/moisture/magnetic damage, secure disposal, protection in transit.
- Fix **roles:** an **Asset Owner** (assigns classification/controls, ensures labelling and authorised access) and an **Asset User** (day-to-day upkeep, maintains CIA, reports weaknesses); **asset registers reviewed half-yearly**.
- **Media procedures:** disable USB ports by default; enable only on approval; scan all media; register incoming/outgoing media; **retain damaged disks and render data non-recoverable**; maintain a **Media Disposal Register** (reviewed quarterly).
- Enclosures include asset registers (information/hardware/software), an Asset Allocation Form and an Asset-Management checklist.

CISO Instruction No. 3/2022 — Physical and Environmental Security (21-01-2022)

Restricts access to premises, critical areas and the Data Centre, and guards against human and environmental hazards. Its mandate:

- Divide premises into **physical zones — Public, Reception, Operations, Security and High Security** — each continuously monitored with escalating access controls; **server rooms secured by biometric access**.

- **Physical entry controls:** access cards for staff on a need-to-know basis; validated visitor entry with register, badges, device declaration and escorting; **no tailgating**; off-hours control; **Data Centre openings monitored round-the-clock by CCTV**.
- **Environmental protection:** firefighting devices, smoke/fire sensors, **fire and earthquake drills (half-yearly)**, flood protection, UPS and emergency lighting.
- **Clear-desk/clear-screen:** lock computers when away, **auto log-off** after inactivity, lock away sensitive papers.
- **Equipment controls:** siting/protection of desktops, hubs, cabling; secure off-premises use of laptops; **secure disposal/re-use** (physical destruction, three-pass wipe or degauss); no removal of assets off-site without authorisation; **storage media never handed to vendors**.
- Fixes the **BISO** role and provides templates (access-card request, visitor entry record, gate passes, fire-inspection and daily checklists).

CISO Instruction No. 2 of 2023 — Role-wise Action Points (dated 17.03.2023)

A consolidated, **role-by-role implementation matrix** for **Pr.CCIT(CCA) regions and Directorates** that maps each post in the hierarchy — from **Pr.CCIT/DGIT down to ITO, ITI/OS/TA/MTS, contractual staff, security personnel and the DDO** — to concrete action points under five domains: **Asset Management, Human Resource Security, Physical & Environmental Security, Incident Management and Risk Management**, each with a **time-line for compliance**. Highlights:

- Every officer must **identify, classify and label** their assets and forward details to the **DDO** to record in **Asset Registers** (created within 15 days; reviewed half-yearly); a **"Do's and Don'ts" (Acceptable Usage) sheet (Annexure 2) pasted at every workstation**.
- **NDAs** signed by all contractors/MSPs within one month; **background-verification** reports within two months; staff **trained** on the ISP (existing staff within a month, new joiners within a week).
- The **CIT(Admin)/LISO** builds an **Asset-Owner code list** (a 7-character Asset ID: 3 letters for city + 4 for office), maintains **risk registers** (filed quarterly to CISO), and runs the regional incident stream.
- The **BISO** gives a **preliminary incident report to the LISO within 24 hours** and routes cyber incidents to **AD/DD/JD(Systems)**; the **CIT(Audit)** conducts the information-security audit.

Why it matters: this instruction is what makes the abstract policy actionable on the ground — it tells each grade *exactly* what to do and by when.

CISO Instruction No. 1(2023) — Investigation Directorates and Central Charges

A specialised role-wise action-point instruction for the **Investigation wing and Central charges**, addressing the acutely sensitive material these offices handle. Its mandate:

- **Information received from foreign jurisdictions (AEOI/treaty data):** original copies moved only in **sealed envelopes marked "Confidential/to be opened by the officer"**; files kept **under lock and key**; **soft data processed only on desktops, never on portable devices**, with encrypted password protection; **no extra copies** created; used **solely for the stated purpose** and **not shared with other agencies without explicit approval**; careful destruction even after case closure to prevent any breach.
- **File handling:** case name written on the **inside cover** (not the top), files carried personally/in envelopes, kept on a side table and **placed upside down** during visitor meetings.
- **Sensitive areas** — LI / NATGRID / **Strong room** / CFL — access **strictly restricted** to authorised employees; **no electronic gadgets (mobiles, pen-drives) inside**; entry/exit logged.
- **Physical security:** boundary wall, no window access, number locks on rooms, rooms cleaned only in the officer's presence, **fire-proof almirahs for seized/impounded material**, and **CCTV covering**

every inch of sensitive areas with a 24-hour control room.

- **Contractual staff:** may carry **no digital/hard-copy material** outside the premises.

CISO Instruction No. 4(2023) — Information Security Audit for CIT(Audit)

Lays down the **methodology for the internal Information Security Audit**. Its mandate:

- The **Information Security Audit is performed annually by the CsIT(Audit)** in every Pr.CCIT(CCA) region; audit of CBDT, its Directorates and attached offices lies with the **CsIT(Audit) of Pr.CCIT(CCA), Delhi**.
- **Three phases, each with a timeline:**

1. **Pre-audit** — the CIT(Audit) intimates the LISO, who supplies the list of offices and BISOs, and an audit plan is prepared (**1 week**);
2. **Audit** — offices are inspected against the Information Security Audit checklists (**1 month**); and
3. **Post-audit** — the final report goes to the LISO with a copy to the **CISO** (**7 days**).

- The **LISO then rectifies non-compliances within 15 days**.
- Provides **four audit checklists** — Asset Management, Human Resource Security, Physical & Environmental Security, and Incident Management — mirroring the four 2022/2023 control instructions.

Why it matters: audit closes the loop — it independently verifies that the policy and instructions are actually being followed, and drives correction of gaps.

Consequences of violation — and the CCS Conduct Rules link

ISP-2020 mandates a **formal disciplinary process for employees and a penal process for contractors/third parties** who breach the policy (Clause 4.7), overseen by the ISC (Clause 2.1.2); internet/policy violations "shall lead to disciplinary action" (8.12). For Government servants this connects directly to the **CCS (Conduct) Rules, 1964** — notably the duties of **integrity, devotion to duty, and maintenance of secrecy of official information** — with penalties imposable under the **CCS (Classification, Control & Appeal) Rules, 1965**. Wilful unauthorised disclosure of taxpayer information can additionally attract the **Official Secrets Act, 1923**, the confidentiality provisions of the Income-tax Act, and (for offences involving external parties) an FIR. The message for every official: a security lapse is not merely a technical slip — it can be a **misconduct with career and legal consequences**.

Legal & procedural references

- **ITD Information Security Policy, 2020** (CBDT, FT&TR Division) — the parent policy (marked "Restricted").
- **CISO Instructions:** No. 1/2022 (HR Security), No. 2/2022 (Asset Management), No. 3/2022 (Physical & Environmental Security), all dated 21.01.2022; **No. 2 of 2023 dated 17.03.2023** (role-wise action points); **No. 1(2023)** for Investigation Directorates & Central Charges; **No. 4(2023)** for CIT(Audit) — Information Security Audit. (Earlier: CISO Instruction No. 1 dated 10.07.2015 and No. 2 dated 27.11.2020.)
- **Information Technology Act, 2000** and **IT (Amendment) Act, 2008**; **CERT-In** guidelines (MeitY); **MHA** information-security guidelines; **Official Secrets Act, 1923**.
- **CCS (Conduct) Rules, 1964** and **CCS (CCA) Rules, 1965**; confidentiality of taxpayer information under the **Income-tax Act, 1961**.
- Alignment with the **ISO/IEC 27001** control framework.

Key Takeaways

- ISP-2020 is itself classified **“Restricted”** and exists to protect the **CIA triad** (Confidentiality, Integrity, Availability) of ITD data; asset criticality is rated as **max(C, I, A)** on a 1–3 scale.
- Five GoI classification levels: **Top Secret, Secret, Confidential, Restricted, Unclassified** — most departmental information is **no higher than Confidential**; classification drives labelling, encryption, access and disposal.
- Governance hierarchy: **ISC** (chaired by **Member I/c FT&TR**) → **CISO** (**Commissioner (Coordination & Systems), CBDT**) → **LISC** → **LISO** (**Commissioner (Admin)**) → **HoDs** → **BISO** (building, ≥CIT rank) / **SISO** (**ADG Systems HQ**) / **PISO** (project); **all exceptions need CISO approval**.
- Access rests on **least privilege + need-to-know**; inactive accounts disabled after **45 days**; screens auto-lock after **5 minutes**; **two-factor authentication mandatory** for critical/remote systems; passwords never shared.
- **Non-government e-mail must not carry classified information; USB ports blocked** by default on sensitive machines; laptops/mobiles need **hard-disk encryption**; defective media is **never** given to vendors.
- Physical security uses **five zones**, **biometric** server-room access, **round-the-clock CCTV**, visitor registers, no tailgating, and **clear-desk/clear-screen**; backups kept **onsite and offsite in a fire-proof safe under departmental control**; **BCP tested bi-annually**.
- Incidents must be **reported promptly to BISO/LISO**; **BISO gives a preliminary report within 24 hours**; cyber incidents escalate to **AD/DD/JD(Systems)**; foreign-treaty-data breaches invoke a special ISC-supervised protocol.
- **Six CISO Instructions** operationalise the policy — **1/2022 (HR Security), 2/2022 (Asset Management), 3/2022 (Physical & Environmental Security), 2 of 2023 (role-wise action points, 17.03.2023), 1(2023) (Investigation/Central charges), 4(2023) (CIT(Audit) Information Security Audit)**.
- Investigation offices apply extra rules: **foreign-jurisdiction data in sealed envelopes, processed only on desktops**, files upside-down before visitors, **fire-proof almirahs for seized material**, strict Strong-room/NATGRID access, no gadgets inside.
- Information-security **audit is annual** (CsIT(Audit)), run in three phased timelines, reporting to LISO/CISO, with non-compliances fixed in **15 days**.
- Violations attract **disciplinary action linked to the CCS (Conduct) Rules, 1964**, penalties under the CCS (CCA) Rules, 1965, and possibly the Official Secrets Act.

Key terms & abbreviations

- **ISP-2020** — ITD Information Security Policy, 2020.
- **CIA** — Confidentiality, Integrity, Availability.
- **ISC / CISO** — Information Security Committee / Chief Information Security Officer.
- **LISC / LISO** — Local Information Security Committee / Officer.
- **BISO / SISO / PISO** — Building / Systems / Project Information Security Officer.
- **ISMS** — Information Security Management System.
- **AUP** — Acceptable Use Policy.
- **NDA / SLA** — Non-Disclosure Agreement / Service Level Agreement.

- **MSP / FMS** — Managed Service Provider / Facilities Management Services.
- **AEOI** — Automatic Exchange of Information (treaty data from foreign jurisdictions).
- **DDO** — Drawing and Disbursing Officer (custodian of asset registers).
- **BCP / DR** — Business Continuity Plan / Disaster Recovery.
- **CERT-In** — Indian Computer Emergency Response Team (under MeitY).
- **CCS Rules** — Central Civil Services (Conduct) Rules, 1964 / (CCA) Rules, 1965.

Part VII — Digital Forensics

18. Digital Forensics in the Income Tax Department

Applicable to: ITO Paper-V, ITI Paper-IV (NOT MS Paper-IV).

Syllabus reference: Digital Forensics — (a) CBDT Digital Intelligence & Analytics Labs (DIALs) standards; (b) Digital Forensics Protocols; (c) Handling of Digital Devices on Initiation of Search and post-search; (d) Disk, Mobile, e-mail and cloud forensics; (e) Cloning, Extraction, Indexing/Clustering, Form 65B / Certificate u/s 63(4)(c) of the Bharatiya Sakshya Adhiniyam, 2023, Chain of Custody, Panchnama and Mazaharnama; and secure handling of seized digital data (CISO Instruction No.1/2023).

Overview

Today almost all evidence of undisclosed income — books, ledgers, WhatsApp chats, e-mails, accounting backups, hawala registers and cloud drives — is **digital**. The Investigation Wing of the Income Tax Department therefore relies on **digital forensics** to identify, preserve, acquire, analyse and present electronic records seized in a **search u/s 132** or impounded in a **survey u/s 133A**. The discipline is governed by CBDT's **Digital Evidence Investigation Manual** (held **mandatory** by the Madras High Court), supported by the Department's **Digital Intelligence & Analytics Labs (DIALs)** for forensic processing, and its end-product must be made **admissible in court** through a certificate now issued under **section 63(4)(c) of the Bharatiya Sakshya Adhiniyam, 2023 (BSA)** (the erstwhile "65B certificate" / Form 65B) — strictly, the certificate is required by s.63(4); clauses (a)–(c) prescribe its contents, and the syllabus refers to it as the s.63(4)(c) certificate. Handled correctly, seized data is legally usable; handled carelessly — for instance by writing to the original, omitting a hash, or breaking the chain of custody — it is liable to be excluded by the court. The subject spans the on-search and post-search protocol, the four forensic branches, and the secure-handling duties imposed by **CISO Instruction No.1/2023** on Investigation Directorates and Central Charges.

Core concepts: digital forensics and electronic evidence

What digital forensics is and why it matters

- **What it is.** Digital forensics is the scientific, court-defensible process of **identifying, preserving, acquiring, analysing and presenting** data held on electronic devices and services so that it can be relied upon as evidence. It is not "using a computer to investigate"; it is investigating the computer (or phone, server or cloud account) itself in a way that does not change the data and that can be independently repeated and verified.
- **Why it matters to the Department.** Modern tax evasion leaves its trail in electronic records — parallel accounts in Tally/Busy, encrypted spreadsheets, chat instructions to accountants, UPI and crypto movements, e-mails arranging accommodation entries. A search that seizes these but mishandles them destroys the very evidence it was meant to capture.
- **Why it matters to the taxpayer.** The same rigour protects the assessee: a properly hashed and custody-tracked image proves the Department did **not** plant, alter or fabricate data, which is a common defence in high-stakes prosecutions.

What electronic evidence is and why admissibility matters

- **What it is.** An "electronic record" (data, record, image, file or output stored, received or sent in electronic form — IT Act, 2000 definition) is treated by law as a **document**. Any printout, copy or output of a computer/communication device is called a **computer output** under BSA s.63.

- **Why admissibility matters.** Seizing data is only half the job; it must survive challenge in court. Electronic evidence is fragile and easily altered, so the law does **not** admit it automatically. It is admissible **without producing the original device** only if the statutory conditions are met and the prescribed certificate accompanies it. If those conditions fail, even genuine, incriminating data becomes legally worthless — hence forensic discipline is a legal necessity, not a technical nicety.

Integrity tools: hashing, write-blocking and forensic imaging

What a hash value is and why integrity matters

- **What it is.** A hash (via **MD5, SHA-1 or SHA-256**) is a fixed-length "digital fingerprint" computed from the entire contents of a file or a whole disk image. The same data always yields the same hash; changing **even one bit** produces a completely different hash.
- **Why it matters.** The hash is the mathematical proof of **integrity**. The examiner computes the hash of the seized media, then of the forensic image, and shows they are **identical** — proving the copy is exact. Re-computing the same hash when the evidence is produced in court proves nothing was altered in between. **SHA-256** is the officially recommended standard and is one of the algorithms named in the BSA certificate form.

What write-blocking and forensic imaging are

- **Write-blocking (what it is).** A hardware or software **write-blocker** sits between the seized media and the examiner's machine and physically/logically **blocks all write commands**, so the original can be read but never changed. It is the tool that operationalises the golden rule "never alter the original."
- **Forensic imaging / cloning (what it is).** A forensic image (clone) is a **bit-by-bit (bitstream) copy** of the entire media — every sector, including deleted, hidden and slack space — not a simple file-by-file copy. Common formats are **E01** (EnCase) and **DD (raw)**.
- **Why they matter.** All analysis is performed on the **image**, keeping the seized original pristine and sealed. Together with hashing, this lets the Department examine, keyword-search and recover deleted data thoroughly while being able to prove the original was untouched.

Documentary safeguards: panchnama, mazaharnama and chain of custody

What a panchnama is and why it matters

- **What it is.** A **panchnama** is the **statutory record of the search** drawn at the premises in the presence of **two independent witnesses (panchas)**. It lists the place, persons present, times of start/end, articles found and seized, and — critically for forensics — each **device (make/model/serial/IMEI)**, the seals affixed, and the **forensic-imaging actions** taken (imaging, hashing).
- **Why it matters.** It is the foundational document proving **how** the digital evidence was obtained and that it was done lawfully and transparently before neutral witnesses. A defective or witness-less panchnama undermines the entire seizure. It is signed by the panchas, the authorised officer and the person searched.

What a mazaharnama is and why it matters

- **What it is.** A **mazaharnama** is a **witness/observation memorandum** — a "panch-witness statement" recording, in the witnesses' own account, what they observed during the proceedings, and the condition and identification of the articles (including devices sealed and imaged).
- **Why it matters.** It **corroborates the panchnama** and independently vouches for the integrity of the seizure and the sealing/imaging of devices, blunting later allegations of tampering or planting.

What chain of custody is and why it matters

- **What it is.** Chain of custody is an **unbroken, documented trail** of **who handled the device or data, when, why, and what was done**. It runs through the successive stages of:

1. seizure;
2. sealing;
3. imaging;
4. DIAL/strong-room storage;
5. analysis; and
6. production in court.

- Every transfer is logged, dated and signed.
- **Why it matters.** Any unexplained gap lets the defence allege the evidence was tampered with or substituted. A clean chain, backed by matching hashes at each stage, is what converts seized data into trustworthy evidence.

The s.63(4)(c) BSA certificate — what it is and why it is essential

- **What it is.** Under **BSA s.63**, computer output is admissible **without the original** if the s.63(2) conditions are met (device under lawful control, used regularly, working properly, output faithfully derived) **and** a **certificate under s.63(4)(c)** — in the form set out in **the Schedule** — is submitted **along with the electronic record at each instance it is produced**. The certificate (a) identifies the record and how it was produced, (b) gives device particulars, and (c) addresses the s.63(2) conditions.
- **Its distinctive features.** The certificate is **dual-signed**: **Part A by the person in charge** of the device/relevant activities (the party), and **Part B by an expert**. Part A records the device type, make/model, serial and IMEI/UIN/MAC/Cloud ID, and the **hash value** with the algorithm used (SHA-1/SHA-256/MD5); a **hash report is enclosed**. In ITD practice the **forensic examiner / DIAL expert** signs Part B.
- **Why it is essential.** It is the successor to **s.65B of the Indian Evidence Act, 1872 (Form 65B)**, which the IEA replaced by the **BSA w.e.f. 1 July 2024**. The operative rule for officers is straightforward: **no s.63(4)(c) certificate → the electronic evidence is not admissible.** The certificate, the hash records and the chain of custody together establish authenticity.

DIALs — Digital Intelligence & Analytics Labs

- **What they are. Digital Intelligence & Analytics Labs (DIALs)** are controlled forensic facilities being set up by CBDT in major investigation charges, staffed by trained personnel using **validated, write-blocked tools** to carry out **cloning, recovery, extraction, indexing and analytics** of seized digital data.
- **Why they matter.** They operationalise the **Digital Evidence Investigation Manual's** standards, provide a secure environment with proper chain-of-custody and strong-room storage, and produce the expert certification (Part B) needed for admissibility. They also feed the Department's **analytics/AI ecosystem (Insight / Project Insight)**, where acquired data is indexed, clustered and correlated to build the evidence trail.

Legal basis for seizing electronic records

- **Section 132(1)(iib), ITA** — empowers the authorised officer to **require any person in possession/control of books of account or other documents maintained as an electronic record to**

afford the necessary facility to inspect them (i.e. provide passwords / decryption / access). This is the statutory hook for accessing and imaging computers, servers and phones during a search.

- **Section 132(1)(iii)/(iv)** — power to **seize** books, documents and other valuable articles; an "electronic record" is a "document" and can be seized, or **cloned** and the clone seized.
- **Deemed seizure (second proviso to s.132(1))** — where it is not practicable to physically remove an article (e.g. a large server), the officer may order that it **shall not be removed/dealt with without prior permission**; in practice the data is **imaged** and the device left in situ or its mirror seized.
- **Section 275B, ITA** — penal consequence (rigorous imprisonment up to **2 years and fine**) for **failure to afford the facility to inspect** electronic records under s.132(1)(iib) — used against those who refuse passwords/decryption.
- **Section 132B** — application/retention of seized assets; retention periods govern how long imaged data/devices are kept.
- **Section 133A (survey)** — books and documents (including electronic records) may be **impounded** (with reasons recorded and approval), and computers/phones inspected; survey does not authorise physical search of premises beyond the place of business.

The digital-forensics protocol

Digital forensics follows a disciplined cycle so that evidence is defensible end-to-end: 1. **Identification** — find all sources of digital evidence. 2. **Preservation** — secure them without altering anything. 3. **Acquisition** — make a verified forensic image and hash it. 4. **Analysis** — examine the image, never the original. 5. **Presentation** — document findings and prepare the s.63(4)(c) certificate.

Each stage is described below.

Stage 1 — Identification

Locate every digital evidence source at the premises: desktops, laptops, servers/NAS, mobiles and tablets, pen drives and external hard disks, memory cards, **DVRs/CCTV**, routers, and — often overlooked — **e-mail accounts and cloud/online storage** to which the devices are logged in.

Stage 2 — Preservation

Secure the scene and stop any change to the data: **do not switch devices on or off carelessly**; photograph screens, cabling and connections; **isolate from the network / Wi-Fi** to prevent remote wiping; and use **write-blockers** so the original is never written to. Volatile data (RAM, live encryption sessions, open cloud logins) is captured **first** where required, because it disappears on power-off.

Stage 3 — Acquisition

Make a **forensic image (clone)** — a bit-by-bit copy — of the storage, and immediately **compute the hash** of both source and image and **verify they match**. This is the moment integrity is locked in.

Stage 4 — Analysis

Examine the **image**, not the original: recover active, hidden, deleted and slack-space data; run keyword/entity searches; trace communications, accounting files and transactions.

Stage 5 — Presentation

Produce documented findings with the exhibits, hash records and the **s.63(4)(c) certificate** so the evidence is admissible in assessment and prosecution.

Cardinal principles of the protocol

- **Do no harm to the original:** act on the original **only when unavoidable** and only by a competent person, who must be able to explain and justify what was done.
- **Integrity by hashing:** every copy is proved identical to the source by matching hashes.
- **Auditability:** every step is documented so that an independent expert could **repeat the process and reach the same result.**

Handling of digital devices

On initiation of search

- **Record before touching:** enter each device in the **panchnama**, photograph it, and note make/model/serial/**IMEI** and physical condition.
- **Cut connectivity:** switch off network/Wi-Fi/mobile data (or use a Faraday bag for phones) to stop remote wiping and incoming changes.
- **Demand access lawfully:** require passwords/decryption keys under **s.132(1)(iib)**; refusal invites **s.275B** prosecution.
- **Do not browse the live device casually** — every click can alter timestamps and metadata.

Handling volatile and live data

Where a machine is found **switched on** (e.g. an open encrypted volume, a logged-in cloud/e-mail session), the examiner captures **volatile evidence first** — RAM contents, active network connections, running processes, open sessions/tokens — because pulling the plug would lose decrypted data and force re-entry of unknown passwords. Only after volatile capture is the imaging/shutdown decision taken.

Imaging on site

Connect the media through a **hardware/software write-blocker**, take a **forensic image**, compute the **MD5/SHA-1/SHA-256 hash** of both source and image, and **verify they match**. Record the hash values in the panchnama/work-notes — this is the evidence that nothing was altered.

Seizure options for digital devices

The authorised officer chooses among: - **Seize the device** itself (sealed, witnessed); - **Seize the clone/image** and leave the device (common where business continuity or bulk data makes removal impractical); or - Pass a **deemed-seizure** order (second proviso to s.132(1)) for bulky servers that cannot practicably be removed.

Post-search handling

- **Transport securely:** anti-static, tamper-evident, sealed packaging; protect from magnetic fields, heat and moisture.
- **Store under custody:** deposit in a **DIAL / strong-room** under an unbroken **chain of custody**, with entries in registers at every transfer.
- **Work on copies only:** carry out detailed extraction and analysis on a **working copy** of the image; keep the master image and original sealed.
- **Retain lawfully:** hold originals/images as per **s.132B** retention limits.
- **Certify before use:** prepare the **s.63(4)(c) certificate** (with hash report) **before** relying on the data in assessment or prosecution.

Cloning, extraction, indexing and clustering

Cloning and hashing

- **Cloning / forensic imaging** — exact bitstream copy (E01/DD) of the media; analysis is done on this, keeping the seized original untouched.
- **Hashing** — identical hashes of original and clone (and again at production) prove **integrity**; a single-bit change breaks the match.

Extraction

- **Extraction** — recovering active, hidden, **deleted** and slack-space data, e-mails, chats, accounting databases, images and **metadata** from the image.

Indexing

- **Indexing** — building a **searchable index** of the extracted content so officers can run keyword/entity searches across terabytes quickly.

Clustering and de-duplication

- **Clustering / de-duplication** — grouping similar/related documents, near-duplicates and e-mail threads so analysts review one representative set instead of millions of files; supports **link/network analysis** to map transactions and persons.

Branches of digital forensics

Disk forensics

Imaging and examining hard disks/SSDs/USBs: file systems, **deleted-file recovery**, registry and OS artefacts, and **accounting-software databases** (e.g. Tally/Busy) and their backups — a frequent source of the "real" parallel books.

Mobile forensics

Extraction (logical / file-system / physical) from smartphones: contacts, call logs, SMS, **WhatsApp/Telegram chats**, photos, app data, location history and **UPI/payment traces**; the **IMEI** is recorded in the panchnama and the phone is kept network-isolated to prevent remote wipe.

E-mail forensics

Analysing **headers**, routing, timestamps, attachments and authenticity; recovering mailbox files (**PST/OST**) to trace correspondence, instructions and accommodation-entry arrangements.

Cloud forensics

Accessing data **stored online / on offshore servers** (webmail, Google Drive/Dropbox, cloud accounting). Acquisition needs **credentials** (sought under s.132(1)(iib)) or lawful service requests; the Manual emphasises capturing **access logs, server logs and user-access records**. Volatility and cross-jurisdiction issues make cloud the most challenging area — **preserve the live session/tokens before logout**, as re-access may be impossible.

Admissibility — Certificate u/s 63(4)(c) BSA, 2023 (erstwhile s.65B / Form 65B)

- Electronic records were earlier admitted under **s.65B, Indian Evidence Act, 1872** (the "65B certificate" / Form 65B). With effect from **1 July 2024** the IEA is replaced by the **BSA, 2023**; **s.63** now governs admissibility and the **certificate** is required under **s.63(4)(c)**, in the form in **the Schedule**.
- A computer/communication-device **output** is admissible **without producing the original** if the **s.63(2)** conditions are met and the certificate **accompanies the record at each instance it is produced**.
- Key change from old s.65B: the BSA certificate is **dual-signed** — **Part A by the person in charge** (party) and **Part B by an expert** — and it records the **hash value(s)** and algorithm, with a **hash report enclosed**. In ITD practice the **forensic examiner / DIAL expert** signs as the expert.

- Practical rule: **no s.63(4)(c) certificate → electronic evidence not admissible.**

Chain of custody, panchnama and mazaharnama in practice

These three documents, each explained earlier in this chapter (see the concept treatment above), together prove lawful, tamper-free handling: the **panchnama** (with two independent panchas) evidences the seizure and imaging; the **mazaharnama** corroborates what the witnesses observed; and the **chain-of-custody** register tracks the sealed exhibits and images through storage, analysis and production. Matching hashes at each hand-over tie the documentary trail to the technical proof of integrity.

Secure handling of seized digital data — CISO Instruction No.1/2023

CBDT's **CISO Instruction No.1 of 2023** lays down **information-security duties for Investigation Directorates and Central Charges**, allocating action points across five domains — **Asset Management, Human Resource Security, Physical & Environmental Security, Incident Management and Risk Management** — to every level from **DGIT(Inv)/CCIT(Central)** down to contractual staff. Key requirements directly relevant to seized digital data:

Asset management and information handling

- Maintain **Asset Registers** of all hardware and software assets; **classify and label** information assets; make handover entries in the asset inventory at every **change of incumbent** (transfer, retirement, suspension, termination, long leave).
- **Portable devices must be password-protected;** sensitive/seized information gathered in the Investigation wing is **not to be retained on portable devices** — soft data is to be **stored and processed on desktops (never on portable devices)** with **encrypted, password protection**.
- **Removable media** (pen drives, hard drives, CDs) must be **scanned for malware** and unnecessary data removed before reuse.
- Information from **foreign jurisdictions** is handled under lock and key, moved in sealed envelopes marked "**Confidential / to be opened by the officer**," used **solely for the stated purpose**, **not shared** without explicit approval, and **no extra copies** created/stored.

Secure media disposal

- Before any media/system is transferred or disposed, **data must be erased so nothing can be recovered** — using **degaussing, physical destruction or secure data wiping** — and the disposal recorded in a **Media Disposal Register**. Any exception triggers an **incident report** under the Information Security Incident Management Procedure. This is critical for **seized-data media** so that recovered evidence is never leaked or resurrected after a case closes.

Physical and environmental security of seized material

- **Strong room / CFL (Central Forensic Lab) / LI / NATGRID areas:** access **strictly restricted** to authorised employees; a **nodal officer** authorises entry case-by-case; entrants log date/time of entry and exit; and **no electronic gadgets (mobiles, pen drives) may be carried into these rooms.**
- **Fire-proof almirahs** for storing **seized/impounded material**; fire extinguishers as per norms; **CCTV** covering sensitive areas, corridors and entry/exit with 24-hour monitoring; buildings secured with boundary walls, locked rooms and controlled delivery/loading areas.

Human-resource security, incident and risk management

- **NDAs** and **background verification** for all contractors/MSPs; access rights removed on contract termination; contractual staff must **not carry any digital/hard-copy material outside** and must return all assets on exit.

- **Incident management** runs through the **BISO / LISO** structure (a **BISO** is nominated per building, an officer not below CIT rank): security incidents are reported and inquired into, cyber incidents escalated to the **Systems** authorities in Pr.CCIT(CCA)'s office, and preliminary reports submitted quickly (BISO within 24 hours).
- **Risk registers** of identified risks are maintained and forwarded **quarterly to the CISO**.

In effect, even after data is forensically imaged, the **CISO regime governs how it is stored, moved, accessed and destroyed**, linking forensic integrity with information security.

Legal & procedural references

- **Income-tax Act, 1961** — s.132 (search & seizure); **s.132(1)(iib)** (afford facility to inspect electronic records / provide access); second proviso to s.132(1) (deemed seizure); **s.132B** (retention of seized assets); **s.133A** (survey / impounding); **s.275B** (penalty for failure to afford access to electronic records).
- **Bharatiya Sakshya Adhiniyam, 2023** — **s.62** (contents of electronic records proved per s.63); **s.63** (admissibility of electronic records), **s.63(2)** (conditions), **s.63(4)(c)** and **the Schedule** (certificate; Part A by person-in-charge, Part B by expert; hash value & algorithm) — replacing **s.65B, Indian Evidence Act, 1872** (Form 65B) **w.e.f. 1-7-2024**.
- **Information Technology Act, 2000** — definitions of "electronic record" / "computer" relied upon.
- **CBDT Digital Evidence Investigation Manual** (held **mandatory** for searches involving electronic evidence — Madras High Court); **CBDT Digital Intelligence & Analytics Labs (DIALs)** standards.
- **CBDT CISO Instruction No.1 of 2023** — information-security duties for Investigation Directorates & Central Charges (asset management, media disposal, physical/environmental security of strong rooms & seized material, HR security, incident & risk management).

Key Takeaways

- Power to demand passwords / facility to inspect electronic records = **s.132(1)(iib)**; refusal is punishable under **s.275B** (up to **2 years RI + fine**).
- A **forensic image/clone** is a **bit-by-bit copy**; analysis is always done on the clone, **never** on the original, using a **write-blocker**.
- A **hash value (MD5/SHA-1/SHA-256)** proves **integrity** — identical hashes of original and clone = unaltered; **SHA-256** is the recommended standard.
- The old **s.65B IEA (Form 65B)** certificate is now the **s.63(4)(c) BSA, 2023** certificate (**w.e.f. 1 July 2024**); it is **dual-signed** (person-in-charge Part A + **expert** Part B) and carries the **hash value & algorithm** with a hash report enclosed; it must accompany the record **at each instance it is produced**. No certificate → **not admissible**.
- **Panchnama** = statutory search record before **two independent witnesses** (lists devices, IMEIs, seals, imaging); **Mazaharnama** = witnesses' observation memo corroborating it; **Chain of custody** = documented, unbroken handling trail.
- Forensic stages: **Identification, Preservation, Acquisition, Analysis and Presentation**; isolate from the network to prevent remote wiping and **capture volatile data first**.
- **Deemed seizure** (second proviso to s.132(1)) is used where a device/server cannot practicably be removed; seizure options are device, clone, or deemed seizure.
- Branches: **disk** (Tally/deleted files), **mobile** (chats/UPI/IMEI), **e-mail** (headers/PST-OST), **cloud** (offshore servers/logs — preserve session before logout); **indexing** makes data searchable, **clustering**

groups duplicates/related data.

- **DIALs** carry out cloning/extraction/analytics and provide expert certification; CBDT's **Digital Evidence Investigation Manual** is **mandatory** for seizing electronic evidence.
- **CISO Instruction No.1/2023:** seized soft data stays on **encrypted desktops, never portable devices**; strong-room/CFL access is restricted (no gadgets inside); seized material in **fire-proof almirahs**; media **securely wiped/degaussed/destroyed** with register entries; incidents handled via **BISO/LISO**.
- The **Income-tax Act, 2025 is NOT in force** for AY 2025-26; apply the ITA-1961 provisions and the BSA, 2023.

Key terms & abbreviations

- **DIAL** — Digital Intelligence & Analytics Lab (CBDT forensic lab).
- **BSA** — Bharatiya Sakshya Adhiniyam, 2023 (replaced the Indian Evidence Act, 1872, w.e.f. 1-7-2024).
- **IEA / s.65B / Form 65B** — Indian Evidence Act, 1872, and its old electronic-evidence certificate.
- **Forensic image / Clone** — exact bitstream copy of digital media (E01 / DD formats).
- **Hash (MD5 / SHA-1 / SHA-256)** — integrity fingerprint of data.
- **Write-blocker** — hardware/software that prevents any write to the original media.
- **Chain of custody** — documented record of who handled evidence, when, why and how.
- **Panchnama** — statutory search-and-seizure record before two independent witnesses.
- **Mazaharnama** — memorandum of witnesses' observations corroborating the seizure.
- **Deemed seizure** — order restraining dealing with an article that cannot be removed (2nd proviso to s.132(1)).
- **Volatile data** — data lost on power-off (RAM, open sessions) captured first.
- **PST/OST** — e-mail mailbox file formats; **E01/DD** — forensic-image file formats.
- **CISO / BISO / LISO** — Chief / Building / Local Information Security Officer.
- **CFL** — Central Forensic Lab (restricted strong-room area for seized material).