Crack the Code

April 2026

An E-Newsletter from CoralMetrix

TABLE OF CONTENTS

Crack the Code

GST MONTHLY UPDATE – APRIL 2026

File DRC-03A before appeal to ensure proper adjustment of payments.

3rd April 2026.

- Taxpayers often make voluntary payments during investigation using Form GST DRC-03. While filing an appeal, the GST portal requires a pre-deposit, even if sufficient payment was already made via DRC-03.
- When a demand order (e.g., Form GST DRC-07) is issued:
    - A Demand ID is created in the Electronic Liability Register (Part II).
    - Payments made using "Payment towards Demand" get auto-adjusted against this Demand ID.

Issue:

Payments made through DRC-03 are not linked to the Demand ID. Hence, they are not considered for pre-deposit calculation during appeal filing.

System behaviour during appeal filing:

- If payments linked to Demand ID ≥ required amount → No additional payment required.
- If payments linked < required amount → Balance payment is mandatory.

Solution:

File Form GST DRC-03A to link DRC-03 payments with the specific Demand ID. Once linked, the amount reflects in the Electronic Liability Register.

Pre-deposit Percentage in the GST Portal

10th April 2026.

While filing an appeal in Form APL-01 on the GST portal, the pre-deposit percentage is auto-populated as 10% in accordance with Section 107(6) of the CGST Act, 2017, and was previously non-editable.

Due to this restriction, taxpayers faced difficulties in cases where the pre-deposit had already been made through other means or where the demand amount was incorrectly reflected under the appropriate head.

To address these issues, GSTN has now made the pre-deposit field editable at the time of filing the appeal, from April 6th, 2026.

This allows taxpayers to modify the pre-deposit percentage as applicable to their specific case and calculate and pay the required amount accordingly while submitting the appeal.

The appellate authority will subsequently verify the correctness of the pre-deposit amount and the mode of payment during the adjudication of the appeal.

Advisory on Re-Computation of Interest under Table 5.1 of GSTR-3B

16th April 2026.

As a facilitation measure for taxpayers and assisting the taxpayers in doing a correct self-assessment, GST Portal auto-calculates interest on delayed filing of GSTR-3B based on the tax liability discharged and tax liability breakup provided in "Tax Liability Breakup, As Applicable" table.

Due to some technical glitch for few taxpayers interest for Feb-2026 period appearing in Table 5.1 of March-2026 period may have been calculated incorrectly without providing benefit of the minimum cash balance available in the Electronic Cash Ledger as per the proviso to Rule 88B(1) of the CGST Rules, 2017.

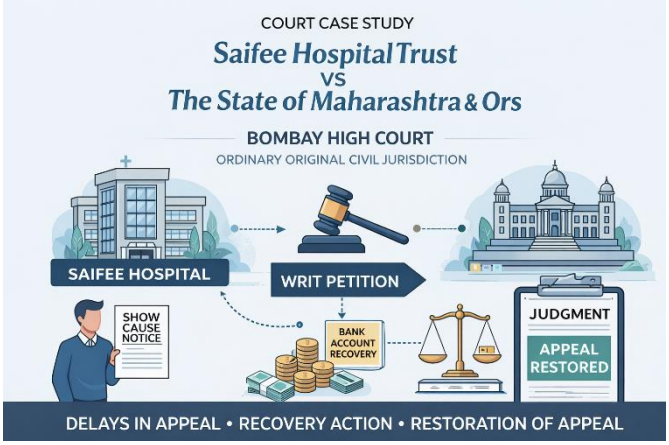
In case any taxpayer observes any discrepancy in the system calculated interest, an option to recompute interest is available on GST Portal.

Editing option of interest field is enabled with a condition of upward modification but not otherwise

Court Room Series

IN THE HIGH COURT OF JUDICATURE AT BOMBAY ORDINARY ORIGINAL CIVIL JURISDICTION

Saifee Hospital Trust vs The State of Maharashtra & Ors`



1. Facts of the Case

- The Petitioner, Saifee Hospital Trust, was subjected to a GST audit for FY 2018–19.
- An Audit Observation Report raised substantial GST demand with interest.
- A DRC-01A intimation and subsequently a Show Cause Notice (SCN) were issued.
- The Petitioner:
    - Denied allegations
    - Filed a detailed reply to SCN
- Order-in-Original (OIO) dated 25.04.2024:
    - Partially confirmed demand:
        - Tax: ₹74.73 lakh
        - Interest: ₹81.67 lakh
        - Penalty: ₹7.56 lakh
- Petitioner filed appeal on 27.08.2024 under Section 107 CGST Act.
- Delay in filing appeal: 1 day beyond condonable period
- Order-in-Appeal (OIA) dated 23.10.2024:
    - Appeal rejected solely on limitation (delay)
- Department initiated recovery proceedings:
    - Issued DRC-13 garnishee notice to HDFC Bank
    - ₹1.53 crore recovered from petitioner's account
- Petitioner approached Bombay High Court under Article 226.

2. Issues for Determination

- Whether delay of 1 day beyond condonable period justifies outright rejection of appeal?
- Whether appellate authority adopted an excessively technical (pedantic) approach?
- Whether such rejection violates principles of natural justice and access to justice?
- Whether High Court should:
    - Interfere in writ jurisdiction
    - Restore appeal for decision on merits
- Whether consequential actions like recovery proceedings survive if appeal rejection is invalid?

3. Arguments of the Petitioner

- Delay was negligible and deserved condonation.
- Delay due to illness of key person handling taxation (Treasurer).
- Appeal rejected on hyper-technical ground.
- No adjudication on merits despite arguable case.
- Huge tax liability fastened without appellate scrutiny.
- Based on procedurally flawed appellate rejection.

4. Arguments of the Respondent (State)

- Appeal filed beyond prescribed limitation under Section 107.
- Appellate authority acted within statutory framework.
- Limitation provisions are mandatory in tax laws.
- State fairly conceded that matter may be remanded for decision on merits.
- Courts must avoid:
    - Mechanical rejection
    - Denial of adjudication on merits
    - Leads to unjust enrichment of State

5.Judgment

The Bombay High Court Quashed and set aside the Order-in-Appeal and Order-in-Original. Also Restored the appeal to appellate authority and Directed for Fresh hearing.

CA SUJATHA G
GST

Legal Series:

Building DPDP Compliance: A Practical Framework for Businesses

The Digital Personal Data Protection (DPDP) Act, 2023 has brought data governance into the core of business operations. While the law defines obligations at a regulatory level, most organizations are still translating those requirements into actionable steps within their own systems.

A common mistake is to approach DPDP as a documentation exercise—updating privacy policies or adding consent clauses.

The framework below outlines how businesses can approach DPDP compliance in a structured and practical manner.

1. Establish Visibility Over Personal Data

The starting point for any compliance effort is visibility.
Most organizations today do not have a consolidated view of personal data. Information is distributed across CRMs, accounting systems, HR tools, spreadsheets, and email communications. In many cases, the same data exists in multiple formats across different teams.
This creates a fundamental risk—organizations cannot control what they cannot see.

The first step, therefore, is to identify where personal data exists, how it is stored, and which systems are involved. This is not merely an IT exercise; it requires coordination across finance, operations, HR, and customer-facing functions.

2. Classify Data Based on Business Context

Once data is identified, it must be understood in context. Not all personal data serves the same purpose. Customer data, employee data, and vendor data each have different usage requirements, sensitivity levels, and regulatory implications.

Without classification, organizations tend to treat all data uniformly—either over-restricting access or leaving it completely open.

A structured classification approach allows businesses to define how data should be handled, who should access it, and what controls are required, based on its relevance and sensitivity.

3. Define Purpose and Justification for Data Collection

A core principle under DPDP is that personal data should be collected only for a specific and lawful purpose.
In practice, however, many organizations collect more data than necessary. Forms are often designed to capture additional fields "just in case," and data collected for one purpose is later reused across functions without clear justification.
DPDP requires a shift in mindset—from convenience-driven data collection to purpose-driven data governance.
Each data point must be linked to a defined use case. If the purpose cannot be clearly articulated, the data should not be collected in the first place.

4. Build Robust Consent Mechanisms

Consent under DPDP is not a formality—it is a foundational requirement.
Organizations must ensure that individuals are clearly informed about:

- What data is being collected
- Why it is being collected
- How it will be used

More importantly, consent must be recorded and retrievable. Businesses should be able to demonstrate when and how consent was obtained.

Equally important is the ability for individuals to withdraw consent. This requires systems that can respond dynamically—ensuring that once consent is withdrawn, data usage is appropriately restricted.

5. Implement Role-Based Access Controls

One of the most common gaps in organizations is uncontrolled internal access to data.
Data is often shared through spreadsheets, downloads, and internal communications without clear boundaries. Over time, this leads to widespread access, with limited accountability.

DPDP requires organizations to define who can access what data, and for what purpose.
This is best implemented through role-based access controls, where:

- Access is linked to job responsibilities
- Sensitive data is restricted
- Data ownership is clearly defined
- This not only improves compliance but also strengthens internal governance.

6. Define Data Retention and Lifecycle Policies

Data retention is one of the least structured areas in most organizations.

Personal data is often stored indefinitely, without any clear policy on when it should be archived or deleted. Over time, this results in large volumes of outdated and unnecessary data.

DPDP requires organizations to define the lifecycle of data—from collection to deletion.
This involves:

- Setting retention timelines based on purpose and regulatory needs
- Establishing archival mechanisms
- Ensuring secure deletion of data once it is no longer required
- Implementing this effectively requires both policy clarity and system capability.

7. Strengthen Data Security Frameworks

Data security is an integral part of DPDP compliance.
Organizations must implement reasonable safeguards to protect personal data from unauthorized access, breaches, or misuse. However, security should not be viewed only as a technical function.
It must be integrated into operational processes.
This includes:

- Controlling system access
- Monitoring data usage
- Ensuring secure storage practices
- Reducing dependency on unsecured formats such as local files and spreadsheets
- A strong security framework reduces both regulatory risk and operational vulnerability.

8. Establish Data Breach Response Mechanisms

Despite safeguards, breaches can occur. What matters is how organizations respond.
DPDP introduces accountability in handling data breaches. Businesses must be prepared to:

- Detect and assess breaches quickly
- Contain and mitigate impact
- Notify relevant stakeholders where required

This requires predefined protocols and clarity on roles and responsibilities.

Without a structured response mechanism, organizations may face both regulatory penalties and reputational damage.

9. Align Vendor and Third-Party Data Practices

Most organizations today rely on external vendors and platforms for operations.

These third parties often process or store personal data—whether through software systems, service providers, or outsourcing arrangements.

Under DPDP, responsibility does not shift to the vendor.
Organizations must ensure that:

- Vendors follow defined data protection standards

- Contracts clearly outline data handling responsibilities
- Data sharing is controlled and monitored

This makes vendor management a critical component of compliance.

10. Build Documentation and Audit Readiness

DPDP compliance must be demonstrable.
Organizations should be able to provide evidence of:

- Data processing activities
- Consent records
- Access controls
- Policies and procedures

This is not only important for regulatory purposes but also for internal governance.
Documentation ensures consistency, accountability, and readiness for audits or reviews.

Closing Perspective

DPDP compliance is not a one-time initiative. It is an ongoing process that requires continuous alignment between legal requirements, operational processes, and technology systems.

Organizations that approach compliance in a structured and phased manner will find it manageable and sustainable.

An important aspect that is increasingly emerging in implementation discussions is the need for a structured consent management mechanism. As organizations scale, managing consent across multiple touchpoints—web forms, onboarding processes, CRM systems, and communication platforms—becomes difficult without a unified system.

This is where a **consent management platform** plays a critical role in ensuring that consent is:

- Captured in a consistent manner
- Stored with proper records
- Linked to data usage
- Easily retrievable and manageable

From an implementation perspective, DPDP compliance is not purely a legal or IT exercise—it requires integration between processes, systems, and governance frameworks.

The focus remains on enabling businesses to move from ad-hoc data handling to structured, system-driven compliance, in a way that is practical to implement and sustainable over time.

Adv.Meenakshi G

AI in Finance: Why Most Implementations Struggle to Deliver Real Value

Artificial intelligence has quickly moved to the center of discussions within finance functions. Across organizations, there is visible momentum—pilot projects, automation initiatives, and increasing interest in using AI for forecasting, reporting, and transaction analysis.

At a surface level, this creates the impression that finance is undergoing rapid transformation.

While adoption is increasing, the actual business impact of AI remains inconsistent. Many organizations have introduced AI into their finance processes, but few have fully integrated it into how decisions are made. The result is a growing gap between capability and outcome.

The Illusion of Progress

In many cases, AI initiatives begin with clear intent. Organizations identify use cases—automating reconciliations, improving forecasting accuracy, detecting anomalies—and deploy tools to address them.

Individually, these initiatives often demonstrate potential.

But over time, a pattern emerges.

The outputs generated by AI systems remain isolated. They are reviewed separately, validated manually, and then incorporated into traditional reporting structures. Finance teams continue to rely on established processes to arrive at final numbers.

In effect, AI becomes an additional layer of analysis rather than an integrated part of the system.

This creates an illusion of progress. The organization appears more advanced, but decision-making remains largely unchanged.

Where the Breakdown Actually Happens

The limitation is rarely in the technology itself. It lies in how AI is introduced into the organization.

Most implementations focus on use cases, not systems.

AI is applied to specific problems without addressing the structure of the underlying data and processes. As a result, the outputs it generates are dependent on inputs that are often inconsistent, fragmented, or manually adjusted.

Finance functions, despite being data-driven, frequently operate with variations in how information is recorded and classified. These variations are managed through reconciliation processes, which are built into reporting cycles.

AI, however, does not operate well in such environments.

When the underlying data lacks consistency, AI outputs require further validation. Instead of reducing effort, they introduce additional layers of review.

This is where many initiatives lose momentum.

The Dependency on Data Structure

A consistent theme across successful implementations is not the sophistication of AI models, but the quality of data they operate on.

Where data is structured, consistently defined, and aligned across systems, AI begins to deliver meaningful outcomes. It can identify patterns across large volumes of transactions, highlight deviations early, and support forward-looking analysis.

Where data is fragmented, the same models produce outputs that are difficult to rely on.

This highlights a critical point.

AI does not fix data problems. It depends on their resolution.

Organizations that recognize this early tend to invest not only in AI capabilities, but also in data governance, system integration, and process standardization.

From Experimentation to Integration

The shift required is subtle but significant.

AI must move from being an experimental layer to becoming part of the core finance system.

This means:

- Embedding AI outputs into regular reporting workflows
- Reducing dependency on manual validation
- Ensuring that insights directly influence decisions

When this happens, the role of finance begins to change.

Instead of spending time reconciling numbers, finance teams can focus on interpreting trends, identifying risks, and supporting business strategy.

Reframing Expectations from AI

There is also a need to recalibrate expectations.

AI is often positioned as a solution that will transform finance on its own. In reality, it is one component of a broader system.

Its effectiveness depends on:

- How well processes are defined
- How consistently data is captured
- How integrated systems are

Without these elements, AI remains underutilized.

With them, it becomes a powerful capability.

A More Grounded Way Forward

Organizations that are beginning to see value from AI are not necessarily those with the most advanced tools, but those that have taken a more structured approach.

They focus on:

- Aligning data across systems
- Standardizing financial processes
- Reducing manual dependencies
- Integrating AI into existing workflows

This approach may appear less aggressive than launching multiple AI initiatives, but it leads to more sustainable outcomes.

Closing Perspective

AI in finance is no longer a question of adoption.

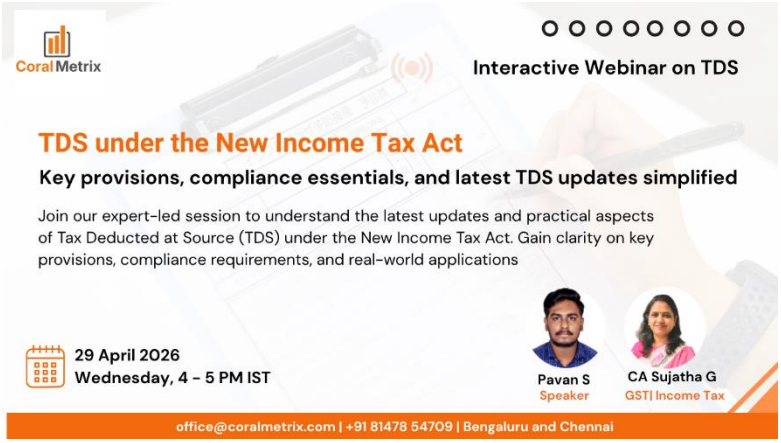
It is a question of integration.

The difference between organizations that experiment with AI and those that benefit from it lies in how deeply it is embedded into their systems.

Where AI is treated as an add-on, its impact remains limited.

Where it becomes part of a structured, integrated finance environment, it begins to influence how decisions are made.

Dipali Kumari



Upcoming Webinar Alert: TDS under the New Income Tax Act

Join us for an informative session on Tax Deducted at Source (TDS) under the New Income Tax Act. This session will cover key provisions, recent updates, and practical insights to help you stay compliant and up to date

Date: 29 04 2026 | Day: Wednesday | Time: 04.00 PM – 05.00 PM

Registration Link: https://meet.zoho.in/nyqn-iyz-gqm

Connect with us

CoralMetrix Advisory
office.coralmetrix@gmail.com
+91 81478 54709
www.coralmetrix.com

Follow us on Social Media