sudeeksha

e-Newsletter from NITIN N & CO., Chartered Accountants

EDITOR'S DESK

Independence is a state of mind.

While we have been celebrating the day we achieved the golden goal of freedom, we need to understand the exact meaning of independence. The day we are able to detach ourselves from the preferences, likes and dislikes while taking decisions; the day we take control of our mind in a way that we respect ourselves and those around; the day we understand that freedom is not absolute and we live in a shared world where we have joint and several rights and duties; the freedom serves the purpose that it should.

Dear CA aspirants, aspire for freedom from the struggles - financial, mental, physical through achieving the goals in a way that does justice to the profession while you collect the membership number from ICAI. Remember that while we perform our duties in office, independence from our self-interest and ideologies and situations is essential to ensure quality. There lies the ultimate result and aim of our efforts...

DISCLAIMER

This newsletter is prepared for general informational purposes only and contains the views, opinions, and interpretations of the author(s). The information provided herein does not constitute professional advice—legal, financial, tax, or accounting—and should not be relied upon as a substitute for consultation with a qualified professional.

While every effort has been made to ensure the accuracy and reliability of the content, the author(s) and the firm do not accept any responsibility for errors, omissions, or misstatements, whether arising from negligence or otherwise. Readers are advised to verify all information independently and exercise their own judgment and discretion before taking any action based on the content of this newsletter.

This newsletter is intended solely for the readers of this publication and may not be reproduced, redistributed, or used in any other form without the express written consent of the author(s). The firm expressly disclaims any liability for any direct, indirect, or consequential loss or damage arising from the use or interpretation of the information provided.

YOUR ROADMAP...

01 **Auditors' Lens**	**Preliminary Engagement Activities – First step in Audit Planning** The essential checks that shape client acceptance, independence and engagement terms before the audit begins.
02 **Tax/ Compliance Corner**	**E-Way Bill 2026: Key Updates Businesses Should Track** Deferred E-Way Bill enhancements, system validation, delivery closure and practical readiness measures. **Undisclosed Sources of Income** Understanding the tax implications and compliance requirements relating to undisclosed sources of income.
03 **Corporate Law Corner**	**SFIO Investigations under Section 212 of the Companies Act, 2013** When SFIO investigations arise, their powers, exclusive jurisdiction, arrest provisions and prosecution framework. **Auditor Appointment During Audit Season** Key considerations and practical guidance on auditor appointments made during the audit season.
04 **Business Compliance**	**Startup Compliance Guide: A Roadmap for Every Entrepreneur** A practical ten-point roadmap covering structure, registrations, books, GST, tax, ROC, payroll, licenses and compliance habits.
05 **Domain Specific Corner**	**What the DPDP Act Actually Looks Like on the Ground** Five practical data-protection scenarios highlighting breaches, consent, children's data, vendors and retention.

AUDITORS' LENS

Preliminary Engagement Activities – First Step in Audit Planning

Before the audit plan is built, the auditor must first determine whether the engagement should be accepted or continued, whether ethical and independence requirements are met, and whether the terms of the engagement are clearly understood.

An audit of financial statements is a complex and systematic process that requires proper planning to ensure that the audit is performed effectively, efficiently and within the required time. Under SA 300, Planning an Audit of Financial Statements, the objective of the auditor is to plan the audit so that it is performed in an effective manner.

Preliminary engagement activities are the initial component of the audit planning process. Their primary goal is to help the auditor identify and evaluate events or circumstances that could adversely affect the auditor's ability to plan and perform the engagement effectively.

Riya Paul

Trainee

Key Elements of Preliminary Engagement Activities

According to auditing standards, preliminary engagement activities consist of three core components:

- Performing procedures regarding the continuance of client relationship
- Evaluating compliance with ethical requirements, including Independence
- Establishing an understanding of terms of engagement

1. Performing procedures regarding the continuance of client relationship

Before accepting a new client or renewing a relationship with an existing one, the audit firm must evaluate whether it is appropriate to do so. This involves:

Evaluating Management Integrity: Assessing the integrity of the principal owners and key management of the client is an important consideration before accepting or continuing an audit engagement.

Assessing the Competence of the Engagement Team: The auditor should ensure that the engagement team has the necessary capabilities and competence to perform the audit engagement. This includes considering whether the team possesses the appropriate knowledge, experience and resources required for the engagement.

Matters arising from current and previous audits: The auditor should consider the implications of matters that have arisen during the current and previous audit engagements. Significant issues identified in previous audits may have implications for the decision to continue the client relationship or because the current audit should be planned.

Communicating with Predecessor Auditors: In the case of an initial audit engagement, where there has been a change of auditors, communication with the predecessor auditor should be made. Such communication may assist the incoming auditor in considering matters relevant to acceptance of the engagement and in understanding matters arising from the previous audit.

2. Evaluating compliance with ethical requirements, including Independence

Independence is fundamental to the auditor's ability to exercise objective and unbiased professional judgment. The auditor's judgment should not be subordinate to the wishes or directions of another person who may have engaged the auditor. The auditor shall continuously evaluate compliance with ethical requirements, including independence, throughout the audit engagement.

The engagement partner should also form a conclusion regarding compliance with the independence requirements applicable to the audit engagement by:

- Obtaining relevant information from the firm to identify and evaluate circumstances and relationships that may create threats to independence.
- Evaluating identified breaches, if any, of the firm's independence policies and procedures to determine whether they create a threat to independence in relation to the audit engagement.
- Taking appropriate action to eliminate the threats or reduce them to an acceptable level by applying suitable safeguards. Where the matter cannot be appropriately resolved, the auditor may need to consider withdrawing from the audit engagement, where withdrawal is permitted by law or regulation and report to the firm for appropriate action.

3. Establishing an understanding of terms of engagement

It is in the interests of both the entity and the auditor that the auditor sends an audit engagement letter before commencement of the audit. The primary purpose of the engagement letter is to avoid misunderstandings regarding the audit engagement.

A clear understanding of the engagement terms helps establish clarity regarding the nature and scope of the engagement and the respective responsibilities of the auditor and the client.

Conclusion: Preliminary engagement activities provide the foundation for the subsequent establishment of the overall audit strategy and development of the audit plan.

Author may be reached at: nncostaff@gmail.com, riapaul327@gmail.com

TAX / COMPLIANCE CORNER

E-Way Bill 2026: Key Updates Businesses Should Track

The proposed E-Way Bill enhancements were initially proposed for implementation from 1 August 2026. The rollout has since been deferred; taxpayers should await official communication before changing systems or compliance processes.

The GST Network (GSTN) has announced proposed enhancements to the E-Way Bill system aimed at improving data accuracy, strengthening audit trails, and enhancing the tracking of goods movement. Among the key proposals are the introduction of mandatory **Ship-to GSTIN** validation in certain transactions and a facility for **voluntary closure of E-Way Bills** after delivery.

Athira Unnikrishnan

Head 1- Assurance & Consulting, HR Manager

Key Proposed Enhancements (Deferred)

1. Mandatory Ship-to GSTIN Validation

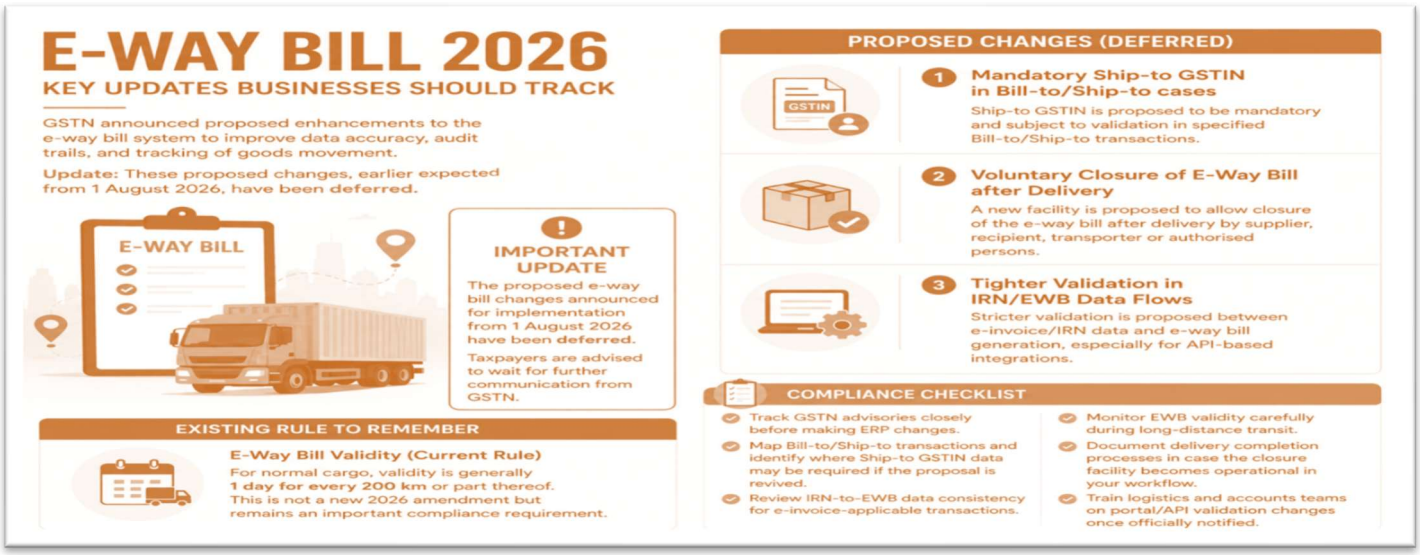
GSTN has proposed making the Ship-to GSTIN mandatory in specified Bill-to/Ship-to transactions. The information would also be subject to system validation. This proposal is expected to improve the accuracy of destination details and strengthen audit trails, particularly for businesses involved in direct deliveries, third-party dispatches, and structured branch transfer models.

2. Voluntary Closure of E-Way Bills

Another proposed enhancement is a facility allowing suppliers, recipients, transporters, and other authorised persons to voluntarily close an E-Way Bill after successful delivery of goods. This feature is intended to provide an additional layer of confirmation for completed transactions and strengthen documentation within the GST ecosystem.

3. Enhanced Validation of e-Invoice and E-Way Bill Data

GSTN has also indicated stronger validation between e-Invoice (IRN) data and E-Way Bill generation, particularly for businesses using API-based integrations through ERP systems, GST Suvidha Providers (GSPs), or Application Service Providers (ASPs). Businesses should therefore ensure that their invoicing and logistics systems maintain accurate and consistent data.



Existing Compliance Requirement

While these proposed enhancements have been deferred, businesses should continue to comply with the existing E-Way Bill provisions. Under the current rules, an E-Way Bill for regular cargo is generally valid for one day for every 200 kilometres or part thereof. Careful monitoring of validity during long-distance transportation remains an important aspect of GST compliance.

Compliance Checklist

To remain prepared for future implementation, businesses should consider the following:

- Monitor official GSTN and CBIC advisories for implementation updates.
- Review Bill-to/Ship-to transactions and identify cases where Ship-to GSTIN may become mandatory.
- Ensure consistency between e-Invoice (IRN) data and E-Way Bill details.
- Monitor E-Way Bill validity to avoid expiry during transit.
- Maintain proper documentation of delivery completion processes.
- Keep ERP systems and logistics workflows ready for future portal validations.
- Train accounts and logistics personnel on upcoming compliance requirements once officially notified.

Conclusion: Reviewing existing E-Way Bill practices, maintaining accurate data, and keeping logistics and finance teams informed will enable a smooth transition whenever the proposals are formally introduced.

Author may be reached at: nncostaff@gmail.com, Unnikrishnanathira123@gmail.com

TAX / COMPLIANCE CORNER

Undisclosed Sources of Income

Sections 68 to 69D deal with different situations where unexplained credits, investments, money, assets, expenditure or certain Hundi transactions may be treated as income when the required explanation or source is not satisfactorily established.

The provisions relating to undisclosed sources of income are important from both tax compliance and documentation perspective. Proper records and supporting evidence are essential where transactions may otherwise fall within the scope of the deeming provisions.

Anjitha Anil

Trainee

1. Cash Credits – Section 68

If any sum is credited in the books of an assessee for a previous year and the assessee does not provide a satisfactory explanation to the Assessing Officer regarding its nature and source, the sum may be treated as income for that previous year.

Where the credited sum is a loan or borrowing, the explanation must also be provided by the person in whose name the credit is recorded and must be satisfactory to the Assessing Officer.

For closely held companies, credits recorded as share application money, share capital or share premium are subject to the applicable requirements regarding satisfactory explanation of the nature and source. The source material also notes the specified exception for amounts credited in the name of Venture Capital Funds or companies registered with SEBI.

2. Unexplained Investments – Section 69

If an assessee makes investments that are not recorded in the books and fails to provide a satisfactory explanation to the Assessing Officer, the value of those investments may be treated as deemed income for that financial year.

3. Unexplained Money, Bullion, Jewellery, etc. – Section 69A

If an assessee is found to own money, bullion, jewellery or other valuable articles not recorded in the books and does not provide a satisfactory explanation regarding their acquisition, the value of those items may be deemed income for that financial year.

4. Investments / Assets Not Fully Disclosed – Section 69B

If an assessee has made investments or owns bullion, jewellery or other valuable articles and the amount spent on these items exceeds what is recorded in the books, the excess amount may be treated as income if no satisfactory explanation is provided

5. Unexplained Expenditure – Section 69C

If an assessee incurs expenditure without a satisfactory explanation of its source, the Assessing Officer can treat such unexplained expenditure as income for that financial year. Further, such expenditure is not allowed as a deduction under any head of income.

6. Borrowing or Repayment on Hundi – Section 69D

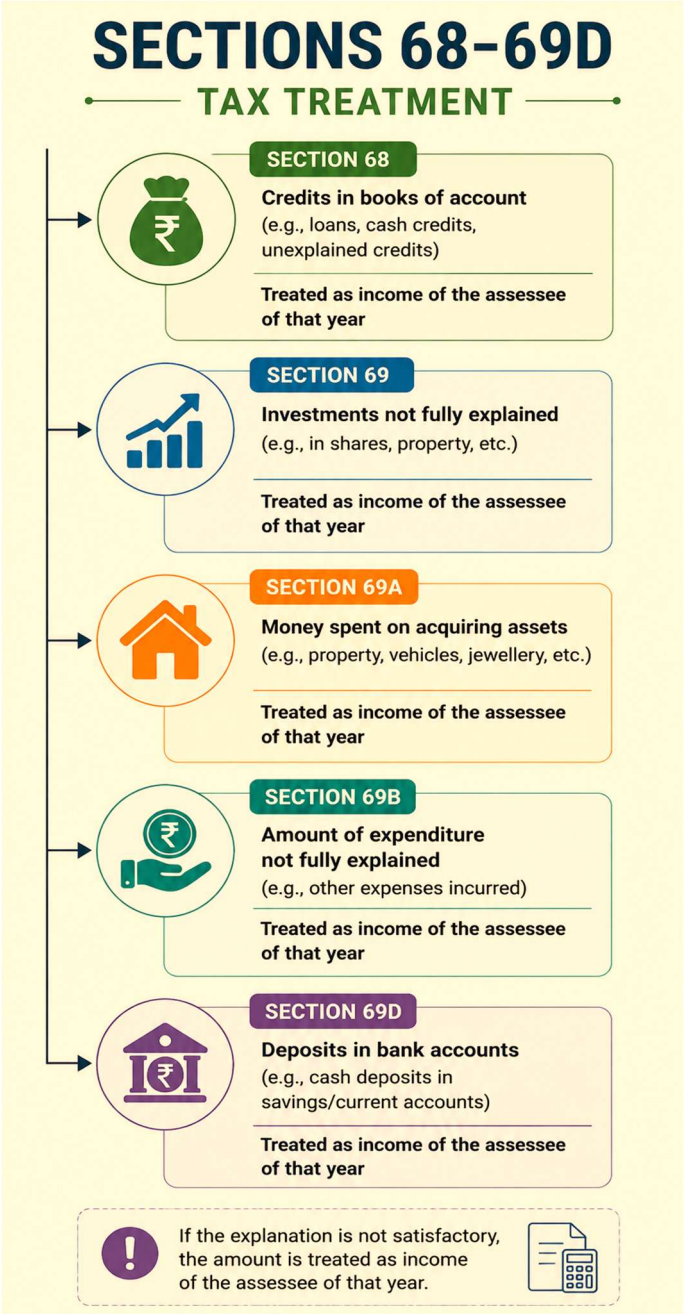
Amounts borrowed on a Hundi, or any amount due thereon, that is repaid otherwise than by an account-payee cheque may be deemed income for the year in which the amount was borrowed or repaid, as applicable.

Where an amount has already been taxed as income upon borrowing, it is not assessed to tax again on repayment. The amount repaid includes the interest component.

Practical Compliance Perspective

- Maintain clear documentary evidence for significant credits appearing in the books.
- Keep supporting documents for loans, borrowings, share capital and share premium transactions.
- Ensure investments and assets are properly recorded in the books of account.
- Maintain evidence supporting the source of significant expenditure.
- Reconcile books with bank accounts and support records regularly.
- Preserve relevant agreements, confirmations, invoices and payment records.
- Review unusual or unsupported transactions before finalizing the return of income.

Proper books alone may not be sufficient where the underlying nature and source of a transaction cannot be satisfactorily demonstrated. Documentation and traceability are therefore critical.



Author may be reached at: nncostaff@gmail.com, anjithanil1526@gmail.com

CORPORATE LAW CORNER

SFIO Investigations under Section 212 of the Companies Act, 2013

A powerful framework against serious corporate fraud: Section 212 empowers the Central Government to assign investigations to the Serious Fraud Investigation Office (SFIO).

Corporate fraud can have a serious impact on companies, investors, and the overall business environment. To deal with cases involving major frauds, the Companies Act, 2013 empowers the Central Government to assign investigations to the Serious Fraud Investigation Office (SFIO) under Section 212.

The SFIO is a specialized agency with experts from various fields, such as law, accountancy, banking, and forensic investigation, to handle complex corporate fraud cases.

Anagha Mariya

Articled Assistant

What is SFIO?

The *Serious Fraud Investigation Office* (SFIO) is a specialized agency under the Ministry of Corporate Affairs that investigates serious and complex cases of corporate fraud. It has experts from different fields such as accountancy, law, banking, taxation, information technology, forensic auditing, and investigation, enabling it to handle complex financial frauds effectively.

When can an SFIO Investigation be Ordered?

The Central Government may order an investigation by the SFIO if it believes that a detailed investigation is necessary. This can happen based on a report from the Registrar or Inspector under Section 208, when a company itself passes a special resolution requesting an investigation, in the public interest, or on the request of any Central or State Government department.

Exclusive Jurisdiction of SFIO

Once a case is assigned to the SFIO, no other Central or State investigating agency can continue investigating the same offence under the Companies Act. If any investigation has already started, it must stop, and all related records and documents must be handed over to the SFIO. The SFIO then completes the investigation and submits its report to the Central Government within the specified time.

Powers of the Investigating Officer

An Investigating Officer appointed by the SFIO has the same powers as an Inspector under the Companies Act. The officer can ask for books of accounts and other records, examine directors, officers, and employees, seek explanations and supporting documents, and require full cooperation from the company. Companies and their employees are legally required to provide the necessary information and assistance during the investigation.

Power of Arrest

Section 212 also gives the SFIO the power to arrest in certain cases. An officer not below the rank of Assistant Director, who is authorised by the Central Government, may arrest a person if there are written reasons to believe that the person has committed an offence covered under this section. After the arrest, the person must be informed of the reasons for the arrest and produced before the Special Court or the jurisdictional Magistrate within 24 hours, excluding travel time.

Bail Restrictions

Offences involving fraud under Section 447 of the Companies Act are cognizable and have strict bail conditions. Bail can be granted only after the Public Prosecutor has been given an opportunity to oppose the application and the Court is satisfied that the accused is not guilty and is unlikely to commit any offence while on bail. However, special consideration may be given to women, minors below sixteen years of age, and persons who are sick or infirm.

Investigation Report and Prosecution

After completing the investigation, the SFIO submits its report to the Central Government. Based on the findings, the Government may initiate prosecution against the company, its directors, officers, employees, or any other persons connected with the fraud. The investigation report filed before the Special Court is treated as a police report under the Code of Criminal Procedure.

Disgorgement of Wrongful Gains

If the investigation shows that any director, key managerial personnel, officer, or any other person has gained an unfair benefit because of fraud, the Central Government may approach the Tribunal to recover such gains. The Tribunal may order the recovery of money, assets, or property obtained through the fraud and may also hold the persons involved personally liable.

Information Sharing

Other authorities such as the Income-tax Department, police authorities, and State Governments are required to share relevant information and documents with the SFIO whenever necessary. Similarly, the SFIO may also share relevant information with these authorities if it is useful for investigations under other laws.

Key takeaway: Section 212 provides a strong legal framework for investigating serious corporate frauds. The Central Government has the power to assign cases to the SFIO, and once assigned, the SFIO has exclusive authority to investigate them. The SFIO has wide powers, including the power to arrest in specified cases, while offences involving fraud under Section 447 are subject to strict bail conditions. The law also allows recovery of wrongful gains from those who benefit from fraud, helping to strengthen corporate accountability.

Section 212 of the Companies Act, 2013 strengthens the fight against corporate fraud by giving the SFIO wide powers to investigate serious cases, collect evidence, arrest offenders in specified situations, and support prosecution. These provisions promote transparency, accountability, and good corporate governance. Companies and their management should maintain proper records, strong internal controls, and comply with legal requirements to reduce the risk of action under this section.

Author may be reached at: nncostaff@gmail.com, anaghamariya480@gmail.com

CORPORATE LAW CORNER

Auditor Appointment During Audit Season

Auditor appointment may appear to be a routine AGM item, but the Companies Act, 2013 provides different procedures for first appointment, AGM appointment or reappointment, casual vacancy and resignation.

As the audit season progresses, the focus generally remains on completing audit procedures, finalising financial statements and issuing the auditor's report. At the same time, companies also move towards the Annual General Meeting (AGM), where appointment or reappointment of the statutory auditor becomes an important compliance matter.

A clear understanding of these provisions can help ensure that the audit and related corporate compliances are completed without procedural gaps.

Theresa Nileena N S

Articled Assistant

1. Appointment of the First Auditor

Under Section 139(6), in the case of a company other than a Government company, the Board of Directors is required to appoint the first auditor within 30 days from the date of registration of the company. If the Board fails to make the appointment within this period, it must inform the members, who must then appoint the auditor at an Extraordinary General Meeting within 90 days. The auditor holds office until the conclusion of the first AGM.

2. Appointment of Auditor at the AGM

Under Section 139(1), the company appoints an auditor at the first AGM, who holds office from the conclusion of that meeting until the conclusion of the sixth AGM, subject to the provisions of the Act, including rotation wherever applicable. The term "appointment" also includes reappointment.

Before the appointment is made, the company should obtain the proposed auditor's written consent and certificate confirming that the proposed appointment is in accordance with the applicable provisions.

3. Reappointment of the Retiring Auditor

A retiring auditor may be reappointed if the auditor is not disqualified, has not given written notice of unwillingness to be reappointed, and a special resolution has not been passed appointing another auditor or expressly providing that the retiring auditor shall not be reappointed.

Before placing reappointment before the members, the company should consider the auditor's eligibility, willingness to continue and the applicable provisions relating to rotation.

4. What If No Auditor Is Appointed or Reappointed?

Section 139(10) provides that where, at any AGM, no auditor is appointed or reappointed, the existing auditor continues to be the auditor of the company. Therefore, the absence of a fresh appointment at the AGM does not automatically result in the office of auditor becoming vacant.

5. When Does a Casual Vacancy Arise?

A casual vacancy arises when the office of auditor becomes vacant before completion of the auditor's term. Under Section 139(8), for a company other than one whose accounts are subject to audit by an auditor appointed by the Comptroller and Auditor-General of India, the casual vacancy is generally filled by the Board within 30 days.

Where the vacancy is caused by resignation, the Board must fill the vacancy within 30 days, and the appointment must also be approved by the company at a general meeting within three months from the date of the Board's recommendation. The auditor appointed to fill the casual vacancy holds office until the conclusion of the next AGM.

6. Resignation of Auditor – Section 140

An auditor who resigns from the company is required under Section 140(2) to file a statement with the company and the Registrar within 30 days from the date of resignation, in the prescribed form and manner. In applicable cases, the statement is also required to be filed with the Comptroller and Auditor-General of India.

The appointment of the new auditor and the resignation-related compliance of the outgoing auditor are separate requirements.

7. Appointment, Reappointment and Casual Vacancy – At a Glance

Particulars	First Auditor	Appointment / Reappointment at AGM	Casual Vacancy
Relevant provision	Section 139(6)	Sections 139(1) & 139(9)	Section 139(8)
Appointing authority	Board; members if Board fails	Members at AGM	Board
Key timeline	30 days from incorporation	At AGM	30 days
Additional requirement	Members appoint if Board fails	Consent, certificate & eligibility	General meeting approval if vacancy is due to resignation
Tenure	Till conclusion of first AGM	As prescribed under Section 139	Till conclusion of next AGM

8. What Should Be Checked Before Appointment?

- **Eligibility** – The proposed auditor should satisfy the eligibility requirements and should not be disqualified under Section 141.
- **Consent and Certificate** – Obtain the written consent of the auditor and the required certificate regarding eligibility and compliance.
- **Auditor Rotation** – Where rotation applies, verify the auditor's tenure and whether reappointment is permissible.
- **Willingness of the Retiring Auditor** – Consider whether the retiring auditor has communicated unwillingness to continue.
- **Correct Appointment Procedure** – Identify whether the matter relates to first appointment, regular appointment/reappointment, or a casual vacancy.
  The applicable procedure may differ in each case.

9. Appointment Does Not End With the Resolution

The compliance process continues even after the appointment is approved. Under **Section 139(1),** the company is required to inform the auditor of the appointment and file the prescribed notice with the Registrar within **15 days of the meeting in which the auditor is appointed**. The Companies (Audit and Auditors) Rules, 2014 prescribe Form ADT-1 for this purpose.

The practical compliance flow can therefore be viewed as:

Before the meeting *→ Eligibility + Consent + Certificate + Required approvals*

At the meeting *→ Appointment / Reappointment approved*

After the meeting *→ Auditor informed + ADT-1 filed + Records updated.*

Auditor Appointment is an important part of the corporate compliance cycle, particularly during the period leading up to the AGM. As the audit season moves towards finalization of accounts and AGM compliances, auditor appointment deserves to be treated as more than just an item on the agenda.

A well-completed audit should be followed by a well-completed compliance process.

Author may be reached at: nncostaff@gmail.com, rojanilin@gmail.com

BUSINESS COMPLIANCE

Startup Compliance Guide: A Roadmap for Every Entrepreneur

Starting a business is exciting, but ensuring compliance with statutory requirements is equally important. Timely compliance helps avoid penalties, improves financial discipline, and builds trust among investors, customers and financial institutions.

Many startups focus on product development and customer acquisition while overlooking legal and financial obligations. A compliance-first approach can provide a stronger foundation for sustainable growth.

Aswathy R Nair

Staff 2- Assurance & Consulting

1. Choose the Right Business Structure

Selecting the appropriate business structure is the first compliance decision for every entrepreneur. Whether it is a Private Limited Company, LLP, Partnership Firm, or Sole Proprietorship, each structure has different legal, tax, and reporting requirements. Choosing the right structure based on the business model and future growth plans can reduce compliance burdens and provide operational flexibility.

2. Complete All Initial Registrations

After incorporation, businesses should obtain essential registrations such as PAN, TAN, and open a dedicated business bank account. Depending on the nature of the business, GST registration, Professional Tax registration, MSME registration, or Startup India recognition may also be required. Completing these registrations at the beginning helps businesses operate without legal hurdles.

3. Maintain Proper Books of Accounts

Accurate bookkeeping is one of the most important aspects of compliance. Every invoice, purchase, expense, and bank transaction should be recorded systematically. Proper accounting not only helps in preparing financial statements but also simplifies tax filings, audits, and business decision-making.

4. Stay Updated with GST Compliance

Businesses registered under GST should issue tax invoices correctly, file returns within the due dates, and reconcile Input Tax Credit regularly. Delayed filings or incorrect reporting can result in interest, penalties, and unnecessary notices from the tax authorities.

5. Ensure Timely Income Tax Compliance

Every business should maintain accurate financial records to compute taxable income correctly. Filing Income Tax Returns on time, paying Advance Tax wherever applicable, and complying with TDS provisions are essential to avoid additional tax liabilities and interest.

6. Meet ROC Filing Requirements

Private Limited Companies and LLPs have statutory filing obligations with the Registrar of Companies. Annual Returns, Financial Statements, and event-based forms should be filed within the prescribed timelines. Regular compliance helps maintain the company's legal status and prevents heavy penalties.

7. Comply with Payroll and Labour Laws

As the business grows and employees are hired, payroll compliance becomes equally important. Employers should ensure timely salary payments, deduction of TDS, and compliance with EPF and ESI provisions wherever applicable. Proper employee documentation also strengthens compliance during inspections and audits.

8. Obtain Necessary Business Licences

Many businesses require additional licences depending on their industry and location. These may include Shop and Establishment Registration, Trade Licence, FSSAI Registration, Import Export Code

(IEC), or other sector-specific approvals. Entrepreneurs should also monitor renewal dates to ensure uninterrupted business operations.

9. Avoid Common Compliance Mistakes

One of the biggest reasons startups receive notices is missing due dates or maintaining incomplete records. Mixing personal and business expenses, delaying GST or TDS payments, and failing to preserve invoices are common mistakes that can easily be avoided through proper planning and regular reviews.

10. Make Compliance a Business Habit

Compliance should not be viewed as a year-end activity. Maintaining a compliance calendar, reviewing statutory deadlines every month, and seeking professional advice whenever required can help startups stay compliant throughout the year. A proactive approach not only reduces risk but also enhances the credibility and long-term success of the business.

Compliance is an investment in the future of every startup. Businesses that maintain proper records, meet statutory deadlines, and follow regulatory requirements are better prepared for expansion, funding opportunities, and sustainable growth. By establishing good compliance practices from the beginning, entrepreneurs can focus on innovation and business development with confidence.

Author may be reached at: nncostaff@gmail.com, nairaswathy1997@gmail.com

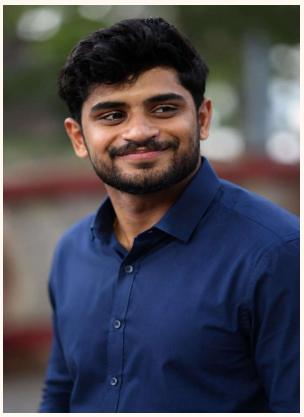
DOMAIN SPECIFIC CORNER

What the DPDP Act Actually Looks Like on the Ground

Five scenarios pulled together from where compliance teams keep tripping up

A colleague asked me last week why so many companies still treat the DPDP Act like a box-ticking exercise for the legal team. Fair question. The Act was passed back in 2023, the rules finally landed in November 2025, and the real deadlines - Consent Manager registration this November, full enforcement by May 2027 - are close enough now that "we'll get to it" is starting to look like a genuine risk rather than a comfortable delay.

There's no library of Data Protection Board rulings to point to yet, since penalties don't bite until 2027 and the Board is still finding its feet. So instead of case law, here are five scenarios stitched together from the kinds of gaps that keep surfacing in gap assessments and audits right now. They're composites, not court transcripts - but anyone who's sat through a vendor review or a breach post-mortem this year will probably recognise the shape of at least one.



Anish C Kamath

Head 2- Assurance & Consulting, IT Manager

What struck me putting these together is how ordinary the failures are. Nobody in any of these situations was trying to misuse anyone's data. They were busy, the paperwork was boring, and the Act's requirements got quietly deprioritized until something forced the issue. That's probably the most useful thing to take from this: compliance gaps rarely announce themselves. They just sit there until a customer complains, a journalist calls, or an audit finally gets around to that part of the business.

Five situations worth learning from

1. The breach that sat in a Slack thread for a week

An online retailer left a cloud storage bucket open to the public for eleven days. Names, phone numbers, delivery addresses - about 40,000 customers' worth. The engineering team fixed it within the hour they found it. What took longer was everyone agreeing on how to describe the incident before telling anyone about it: legal wanted one version, comms wanted another, and the debate ran on for the better part of a week.

That's the part that actually creates exposure. Section 8(6) puts the duty to prevent breaches on the fiduciary, and Rule 7 expects intimation to the Board and to affected users without unreasonable delay. A misconfigured bucket is a technical failure; a week-long argument about phrasing is a governance one, and it's the governance failure that regulators will care about.

By the time the company finally sent notifications, customers had already started finding out on their own - a few screenshots on social media, the usual pile-on, and a spike of complaints landing on a grievance officer who wasn't set up to handle that volume. None of that would have changed the underlying breach, but it changed how it looked.

Worth doing now: write the breach notification template before you need it and decide in advance who has the authority to send it.

2. One checkbox, four different consents

A lending app bundled the loan agreement, marketing opt-in, data sharing with recovery agents, and access to the phone's contact list into a single checkbox. You couldn't get the loan without agreeing to all four. It's a pattern that's everywhere in Indian apps, honestly, and it's exactly what Section 6 is written against - consent has to be specific and unbundled, not one blanket "I agree."

The company only caught it because they were mapping their flows for Consent Manager readiness ahead of the November deadline. If they hadn't been looking, it likely would have sailed through unnoticed for another year.

Worth doing now: pull marketing and any non-essential data use out of the core consent flow and make them genuinely optional.

3. A school app, a targeted ad, and an angry parent

A homework-tracking tool used in several schools collected attendance and grades, and in some cases home addresses, on the assumption that the school's enrolment paperwork already covered consent. It didn't - not under Section 9, which requires verifiable parental consent for a child's data, full stop, and separately bans profiling or targeted advertising aimed at children regardless of what anyone agreed to.

The problem became visible the way these things usually do: a parent got an ad that referenced their kid's school and complained loudly. Turns out relying on someone else's consent form is a habit a lot of ed-tech products have picked up from the GDPR era, and it doesn't transfer cleanly to how DPDP treats children's data.

Worth doing now: get direct, verifiable parental consent—don't inherit it from a school, an employer, or anyone else.

4. The WhatsApp vendor nobody actually vetted

A diagnostics chain started sending test results to patients over WhatsApp through a third-party notification vendor, to speed things up. Sensible idea. Except the vendor kept every report on its own servers indefinitely, unencrypted, and nobody at the diagnostics chain had ever signed a data processing agreement with them - the relationship had just... started, two years earlier, and nobody circled back.

Section 8(2) is unambiguous that using a processor doesn't transfer the liability. If the vendor mishandles the data, the fiduciary still owns the consequences. This is probably the most common gap out there: fast partnerships, slow paperwork.

Worth doing now: no vendor touches personal data without a signed DPA, defined retention limits, and someone having actually looked at their security practices.

5. An exit interview turns into a data request

A departing employee asked HR for a copy of everything the company held on them, and asked for it to be deleted six months after they left. Reasonable requests - Sections 11 and 12 give any Data Principal the right to access and erasure. HR's honest answer was that they didn't know what could be deleted, because nobody had ever written down what needed to be kept for statutory reasons versus what was just sitting there out of habit.

They worked it out, eventually, by building a retention matrix on the spot under a deadline. It's not a great way to discover you don't have one.

Worth doing now: put a retention schedule together before the request arrives, not while you're answering one.

The pattern underneath all five

None of these are stories about bad intent. Nobody set out to break the law. They're stories about paperwork that never got written, vendor relationships that outran the contracts backing them, and consent screens designed for conversion rates rather than compliance. That's a more mundane story than a data-protection scandal, but it's the one that's actually playing out in most organisations right now.

- The Data Protection Board runs on complaints in its early phase - one annoyed customer, parent, or ex-employee is enough to trigger a look.
- Consent Manager registration opens 13 November 2026. If your consent flow is still bundled, that's a real deadline, not a suggestion.
- Full enforcement, penalties included, lands 13 May 2027 - plenty of runway, but every scenario above shows how fast the cracks show up once someone actually checks.

A short list to start with

- Map where personal data actually lives - collection points, storage, every vendor it passes through.
- Split consent by purpose; nothing non-essential should be bundled with the thing the user actually wants.
- Get DPAs signed with every processor, with real retention and security terms, not boilerplate.
- Write the breach notification playbook now, including who's authorised to send it.
- Build a retention schedule so access and erasure requests aren't improvised.
- Name a grievance officer (or DPO, if you're a Significant Data Fiduciary) and make sure that person is actually reachable.

Practical takeaway: data-protection compliance is less about a one-time policy exercise and more about building repeatable operational processes.

Author may be reached at: nncostaff@gmail.com, anishckamath191@outlook.com

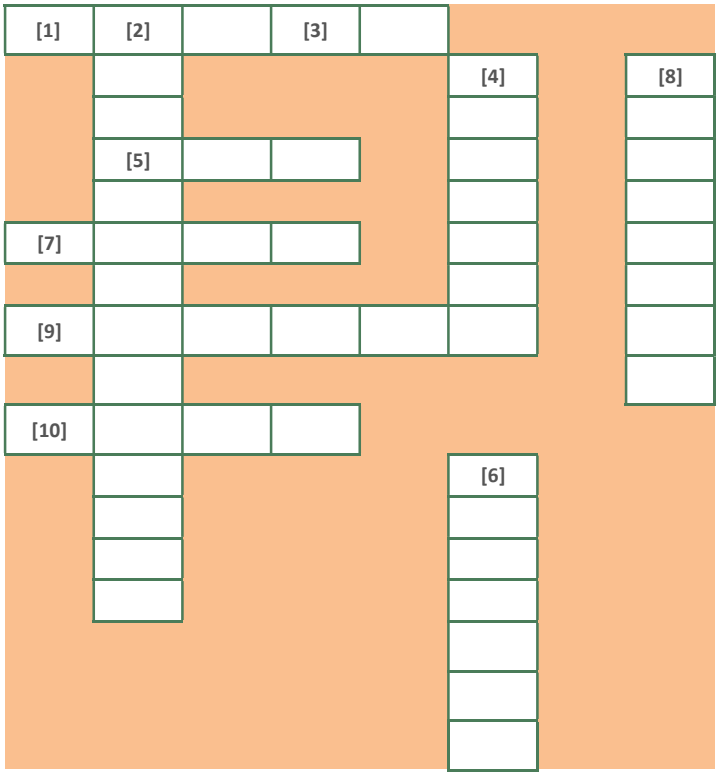
Happy Independence Day

Let us celebrate the spirit of freedom that inspires us to dream, grow and move forward. May the values of unity, integrity and responsibility continue to guide our nation. Let us honour the sacrifices of those who shaped our journey towards independence. Together, let us contribute to a stronger, progressive and prosperous India. Wishing everyone a very Happy Independence Day! Jai Hind!

MEMORY BOX

SESSIONS...

CROSSWORD PUZZLE



ACROSS CLUES		
#	Clue	Length
1	A person who acts on behalf of another person, often subject to tax under representative assessee rules	5
3	Under GST, the document issued by a registered person to transfer tax credit internally	3
5	Materiality concept in auditing is governed by SA ____	3
7	Type of duty levied on imports to protect domestic industry against unfair low prices	3
9	Systematic process of verifying that inventory matches accounting records	5
10	A resident individual under FEMA must be in India for more than ____ days in preceding FY	3

DOWN CLUES		
#	Clue	Length
2	Professional skepticism is an attitude of a ____ mind	11
4	Costing method used when products pass through continuous operational stages	7
6	Under FEMA, transactions on account of trade/services fall under ____ account	7
8	Unabsorbed depreciation can be carried forward for an ____ period	8

The answers from last month's crossword are also included for reference to help you revise and track your progress.

V	F	E	M	A	E
O			C		P
U	C	P	A	N	O
C	I				R
H	A	U	D	I	T
E					
R	T	D	S		
		G	S	T	
			R	O	C

sudeeksha

e-Newsletter from NITIN N & CO., Chartered Accountants

THANK YOU

SCAN THE FOR ME