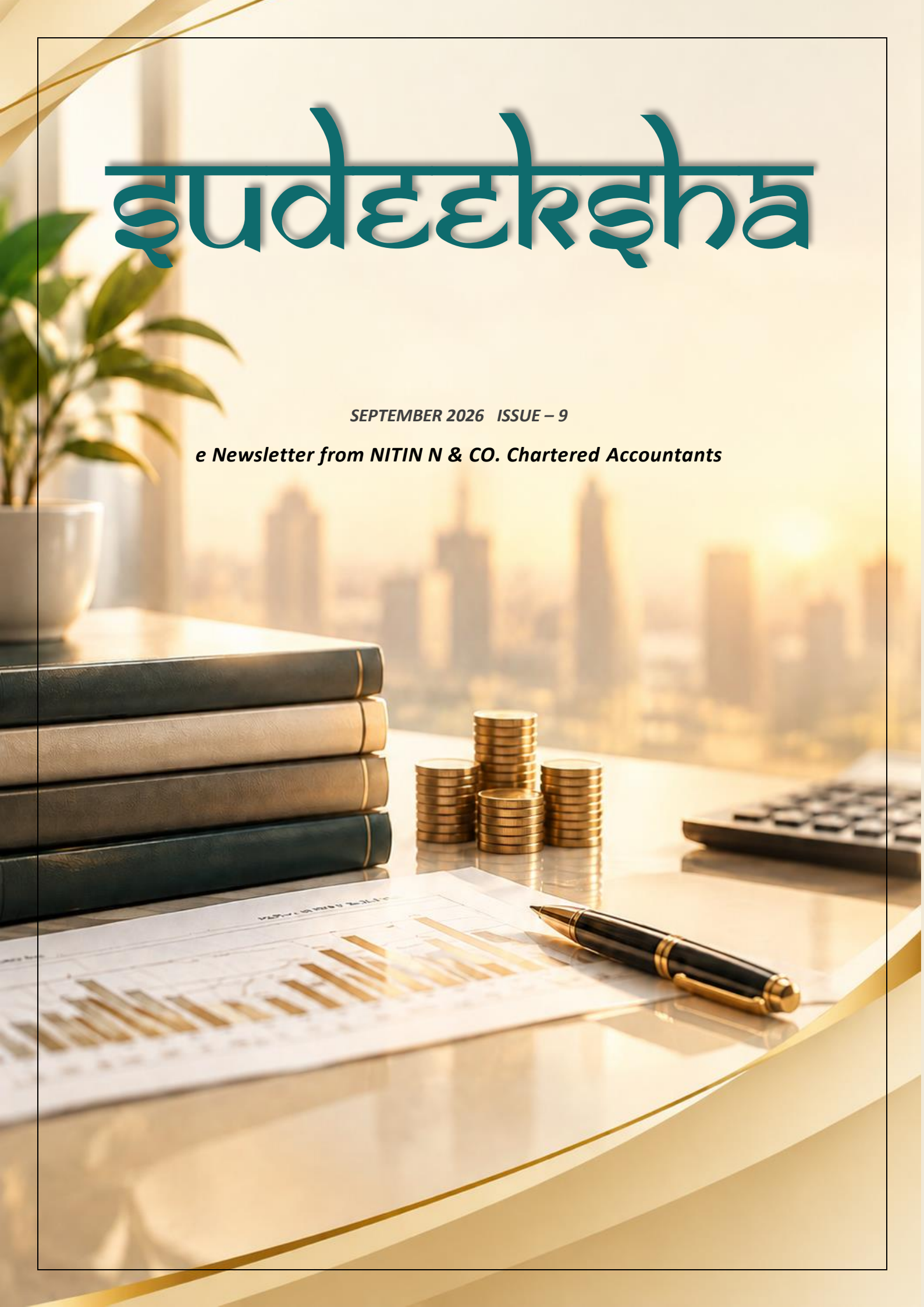


इएवईएरइहव

SEPTEMBER 2026 ISSUE – 9

e Newsletter from NITIN N & CO. Chartered Accountants



INSIDE

This edition brings together timely insights across law, GST, audit, finance, and taxation. It explores the emerging intersection of Artificial Intelligence and Law, practical aspects of Composition Levy and GST Notices, the significance of Forensic Accounting and International Standards on Auditing, and the fundamentals of Options. The edition also examines the important distinction between Tax Planning and Tax Evasion. With a focus on practical relevance and contemporary professional developments, these articles aim to equip readers with valuable insights to navigate today's evolving professional landscape.

FROM THE DESK

September is the month of responsibility for Chartered Accountants. It is considered as the peak season where the efforts over several months culminate into a fruitful exercise of statutory compliance, value addition and personality development.

This month teaches the students many things much beyond what the written material in the form of books teach. It is a deep dive into the spirit behind the words, figures and documents than the mere words and numbers. It is a sense of stewardship and trust that form part of our profession and based on which the reputation of a Chartered Accountant gets weighed upon.

Trust in this sense should be interpreted as the sense of responsibility that the attestation authority brings. Our signature is the basis of trust that we have exercised due procedures. It is the best month to repay the faith that your mentors and employers placed in you as an assistant. It is a reminder that many seniors walked this path earlier who made ICAI what it is today. Let us uphold the dignity; upgrade the standards, upskill the competence; of self and profession.

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.

EDITION OVERVIEW

1	GST Notices: What Businesses Should Do When They Receive One	Page: 5-7
2	Composition Levy	Page: 8-9
3	Following the Money: When Forensic Accounting Steps In	Page: 10-12
4	ICAI's New Information Systems Audit Standards	Page: 12-14
5	Options Uncovered: Understanding the Right to Buy or Sell	Page: 15-18
6	When AI Goes Wrong, Who Answers for It?	Page: 19-22
7	Tax Planning vs Tax Evasion: Understanding the Difference	Page: 23-24
8	Crossword	Page: 25
9	Memory Box	Page: 26

ATHIRA UNNIKRISHNAN

HEAD-1 ASSURANCE AND CONSULTING

Email ID: unnikriishnanathira123@gmail.com



GST Notices: What Businesses Should Do When They Receive One

A Practical Guide from Notice Receipt to Effective Response

Receiving a GST notice can be concerning, but it does not necessarily mean that a tax liability has been established. Notices may be issued to seek clarification, verify information, reconcile differences or examine compliance.

What matters is how promptly and appropriately the taxpayer responds.

Step 1. Understand the Notice

The first step is to read the notice carefully and identify:

- | | |
|---|--|
| <ul style="list-style-type: none"> • The GSTIN and taxpayer details • Relevant financial year and tax period • Section under which the notice is issued • Nature of the discrepancy or information sought | <ul style="list-style-type: none"> • Tax, interest or penalty involved, if any • Documents or explanation required • Date by which the response must be submitted |
|---|--|

Different GST communications serve different purposes, so the nature of the notice determines the appropriate course of action.

Step 2. Identify and Verify the Issue

Common reasons for GST notices include:

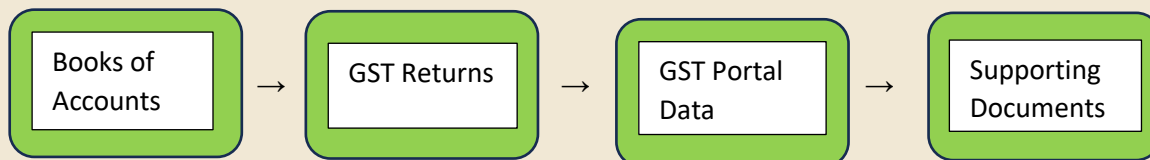
- | | |
|--|---|
| <ul style="list-style-type: none"> • Differences between GSTR-1 and GSTR-3B • Mismatches between books and GST returns • Input tax credit differences involving GSTR-2B | <ul style="list-style-type: none"> • E-invoice or e-way bill discrepancies • Short payment or non-payment of tax • Incorrect or excess input tax credit • Interest or late fee issues • Registration-related discrepancies |
|--|---|

GST INSIGHTS

A discrepancy reflected in departmental data does not automatically establish a tax liability. The underlying transactions and records must first be verified.

Step 3. Reconcile Before Responding

The response should be based on a proper reconciliation of:

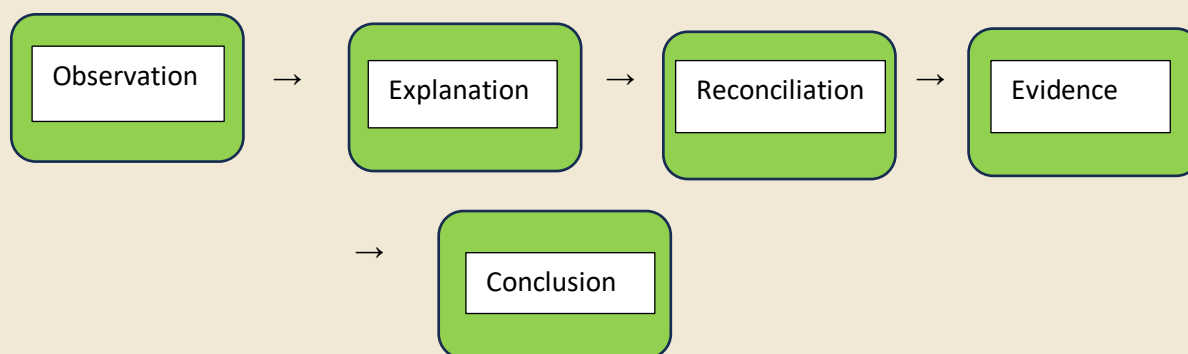


For example, a turnover difference may arise because of exempt or non-GST supplies, exports, credit notes, advances or accounting adjustments. Similarly, an input tax credit difference should be examined against purchase records, tax invoices and GSTR-2B.

A clear reconciliation can often explain the difference and establish the taxpayer's position.

Step 4. Prepare a Point-wise Response

A well-drafted response should address each observation separately and follow a simple structure:



Supporting documents may include:

- | | |
|---------------------------------------|--|
| • Sales and purchase registers | • Ledger extracts |
| • Tax invoices and credit/debit notes | • Bank statements |
| • GST returns and portal data | • Payment challans |
| • E-invoices and e-way bills | • Relevant agreements or other records |

Documents should be linked to the specific explanation rather than uploaded without context.

Step 5. If the Liability Is Correct

Not every notice results from an error by the department. If reconciliation confirms a short payment or other compliance lapse, the taxpayer should determine the applicable tax, interest and penalty implications and take the appropriate corrective action.

Early identification and resolution can help prevent the matter from becoming more complicated.

Step 6. If You Disagree With the Notice

Where the proposed liability is not correct, the response should clearly explain the factual and legal basis for disagreement.

GST INSIGHTS

Instead of simply stating that the demand is incorrect, the taxpayer should support the position with relevant records, reconciliations and, where appropriate, applicable legal provisions or judicial precedents.

Step 7. Do Not Miss the Deadline

A notice should never be ignored or left until the last minute. Failure to respond within the prescribed time can result in further proceedings based on the information available with the department.

After submission, retain the notice, response, supporting documents and proof of submission for future reference.

GST Notice Response Checklist

- | | |
|---|--|
| <ul style="list-style-type: none"> ☐ Identify the issue and relevant tax period ☐ Check the response deadline ☐ Reconcile the figures with books and GST records ☐ Verify the applicable provisions | <ul style="list-style-type: none"> ☐ Gather relevant supporting documents ☐ Address every observation point-wise ☐ Review the response before submission ☐ Preserve the acknowledgement and complete records |
|---|--|

Common Mistakes to Avoid

- **Ignoring the notice:** Even a seemingly minor discrepancy requires attention.
- **Responding without checking the facts:** Always reconcile the figures before accepting or disputing an observation.
- **Giving a generic reply:** Address each issue specifically.
- **Submitting documents without explanation:** Evidence is effective only when it supports a clear explanation.
- **Making premature admissions:** Verify the facts and applicable provisions before accepting a proposed liability.

Conclusion

A GST notice is best handled through a structured approach: **understand the issue, verify the facts, reconcile the records and respond with evidence.** Regular reconciliation of books, GST returns and portal data can also help businesses identify discrepancies before they result in departmental queries.

Prompt action and a well-supported response can make a significant difference in resolving GST matters efficiently.

ANJITHA ANIL

TRAINEE

Email ID: anjithaanil1536@gmail.com



COMPOSITION LEVY

The Composition Levy under GST is a simplified tax scheme for small taxpayers, allowing them to pay tax at a fixed percentage of turnover instead of regular GST rates, with reduced compliance requirements. It is optional, available to businesses with turnover up to ₹1.5 crore (₹75 lakh in specified states) but comes with restrictions such as no input tax credit and limited eligibility.



Key Features of Composition Levy

- Legal Basis: **Section 10** of the **CGST Act, 2017** (with Rules 3–7 of CGST Rules).
- Purpose: Reduce compliance burden for small businesses by avoiding complex return filings and invoice matching.
- **Optional Scheme:** Businesses can choose to opt in if eligible.

Eligibility & Thresholds

➔ Turnover Limit:

₹1.5 crore (aggregate turnover in preceding financial year).

₹75 lakh for specified states (Arunachal Pradesh, Manipur, Meghalaya, Mizoram, Nagaland, Sikkim, Tripura, Uttarakhand).

➔ Eligible Persons:

- ❖ **Manufacturers** (except notified goods like ice cream, pan masala, tobacco).
- ❖ **Traders** (suppliers of goods).
- ❖ **Restaurants** (not serving alcohol).
- ❖ Certain **service providers under Section 10(2A)** with turnover up to **₹50 lakh**.

GST INSIGHTS

 Not Eligible:

- ❖ **Casual/non-resident** taxable persons.
- ❖ Businesses making **inter-state outward supplies**.
- ❖ **E-commerce sellers** (through operators liable for TCS).
- ❖ Suppliers of **non-taxable goods**.

Tax Rates under Composition Scheme

Category	Rate of Tax	Notes
Manufacturers (except notified goods)	1% CGST + 1% SGST = 2%	Not for ice cream, pan masala, tobacco
Restaurants	2.5% CGST + 2.5% SGST = 5%	Only non-alcoholic restaurant services
Traders/Other suppliers	0.5% CGST + 0.5% SGST = 1%	On turnover of taxable supplies
Service providers (Sec 10(2A))	3% CGST + 3% SGST = 6%	For turnover up to ₹50 lakh

Compliance Requirements

- Returns: Quarterly payment (CMP-08) + Annual return (GSTR-4).
- Invoice: Must issue a Bill of Supply (not tax invoice).
- Input Tax Credit: Not available under composition levy.
- Tax Payment: On turnover in state/UT, not on value-added.

Limitations & Risks

- Cannot collect tax from customers (must absorb tax in pricing).
- No input tax credit → higher effective cost if dealing with GST-registered buyers.
- Restricted business expansion (e.g., inter-state supply not allowed).
- Not suitable for businesses with high input tax credit needs.

AUDITOR'S LENS

ANAGHA MARIYA

ARTICLED ASSISTANT

Email ID: anaghamariya480@gmail.com



Following the Money: When Forensic Accounting Steps In

When financial records are properly maintained and the books balance, it may seem that everything is in order. However, accurate bookkeeping and balanced accounts do not necessarily mean that every transaction is genuine, properly authorised, or free from irregularities.

This is where **forensic accounting** plays an important role. Unlike a routine audit, which primarily focuses on expressing an opinion on financial statements, forensic accounting involves a detailed examination of financial information to **identify irregularities, answer specific questions, establish facts, and support disputes or legal proceedings.**



Forensic Standards in India

As forensic accounting gained importance, ICAI introduced **the Forensic Accounting and Investigation Standards (FAIS)** through a series of standards and exposure drafts beginning in 2020. The revised FAIS were issued on **1st July 2023** and became mandatory for forensic engagements conducted on or after that date.

The standards provide guidance on key areas such as fraud risk, evidence, documentation, data analysis, digital evidence, reporting and quality control, helping ensure that forensic work is carried out in a consistent and professional manner.

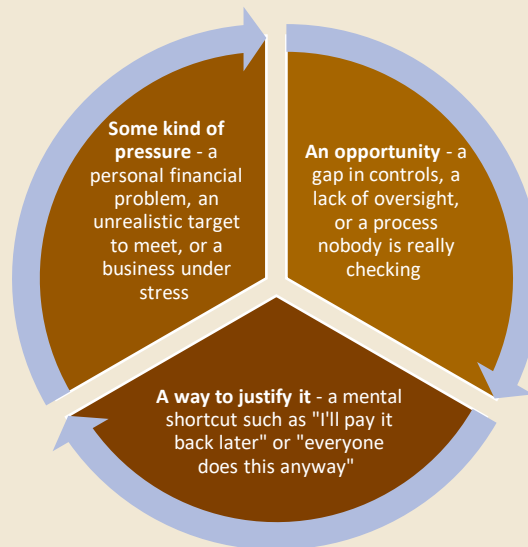
The Importance of Independence and Objectivity

The effectiveness of a forensic accounting engagement depends on an independent, evidence-based approach. The objective is not to prove fraud, but to establish what the available evidence shows. Financial records, bank transactions, invoices, agreements and electronic records may need to be examined and connected to understand the facts clearly. In India, the **Forensic Accounting and Investigation Standards (FAIS)** issued by ICAI provide a structured framework to ensure that such engagements are conducted consistently, fairly and reliably.

Why Does Financial Wrongdoing Happen in the First Place?

Before looking at when to call in a forensic accountant, understand why such situations arise at all. Interestingly, most cases of financial wrongdoing tend to share three ingredients:

AUDITOR'S LENS



When **all three come together**, even people who would otherwise never think of themselves as dishonest can end up crossing a line. It's equally about reducing undue pressure on people and building a culture where cutting corners doesn't feel justifiable in the first place.

When Should a Business Consider Forensic Accounting?

1. Inventory differences that cannot be explained

Repeated differences between physical stock and accounting records can indicate more than an ordinary accounting error. A forensic review can trace purchases, receipts, movements, sales and

consumption of inventory to identify the source and nature of the discrepancy.

2. Disputes between partners, promoters or shareholders

Financial disagreements can become particularly difficult when the parties have different

views about the movement or utilisation of funds. An independent examination of bank accounts, books of account and supporting documents can help establish the actual flow of funds and provide an objective basis for resolving the dispute.

3. Concerns regarding utilisation of borrowed funds

Where questions arise regarding the utilisation of loans or other borrowings, an independent review can help establish whether the funds were applied for the intended purposes. Identifying and addressing such concerns at an early stage may help management take appropriate corrective action.

4. Complaints or whistleblower allegations

an allegation of financial misconduct does not, by itself, establish that wrongdoing has occurred. However, it should not be disregarded either. Forensic procedures can help examine the underlying transactions, verify supporting evidence and determine whether the allegation is supported by facts.

5. Unusual transactions or unexplained financial patterns

Sometimes there may not be one obvious red flag. Unusual payment arrangements, unexplained changes in margins, transactions with unfamiliar vendors, related-party concerns or inconsistencies between financial and operational information may warrant closer examination.

AUDITOR'S LENS

Isn't This Just a Stricter Version of an Audit?

It's a common question, and worth clearing up because the two are genuinely different jobs.

AUDIT	FORENSIC ACCOUNTING	INVESTIGATION
Examines financial statements as a whole	Begins with a specific concern, discrepancy, dispute, or allegation	Focuses on a suspected legal, ethical, or contractual violation
Uses largely sample-based testing	Involves detailed examination of relevant transactions	Seeks to establish whether the specific violation occurred
Provides an audit opinion	Produces documented findings and evidence	Establishes facts through focused inquiry
Focus: Overall financial reporting	Focus: Evidence and facts	Focus: Specific suspected violation

Benford's Law: Finding the Unusual

Benford's Law analyses the distribution of leading digits in large sets of financial transactions and can help identify unusual patterns. In an **audit**, an unusual pattern may indicate an area requiring further testing. In a **forensic engagement**, it can serve as an **investigative lead**, prompting deeper examination of invoices, vendors, approvals, bank payments, and other evidence. The key is that an unusual pattern **does not prove manipulation**; it signals the need for further investigation.

Forensic Accounting Is Not Limited to Fraud

Forensic accounting is often associated with fraud investigations, but its application is much wider. A properly conducted review can help an organisation:

- Determine whether a suspected irregularity actually occurred
- Identify weaknesses in financial and internal control systems
- Trace and quantify financial losses, where applicable
- Provide management with reliable information for decision-making
- Establish an objective and well-documented record for use in disputes or proceedings

In some cases, the conclusion may be that the initial suspicion was not supported by the evidence. That too is a valuable outcome, as it enables management to make decisions based on facts rather than assumptions.

Forensic accounting extends beyond investigating financial problems; it serves as a proactive risk-management and advisory tool, helping businesses identify irregularities early, assess concerns objectively, and make informed decisions.

AUDITOR'S LENS

ANISH C KAMATHHEAD- 2 ASSURANCE AND CONSULTING, IT
MANAGER

Email ID: anishckamath191@outlook.com



ICAI's New Information Systems Audit Standards

A practical look at the ISAS compendium and what it changes for audit engagements



In April 2026, ICAI's Digital Accounting and Assurance Board (**DAAB**) released the Compendium of Information Systems Audit Standards, or ISAS - the first formal set of standards written specifically for IS audit work. It had been circulating as an exposure draft since December 2025, so the direction wasn't a surprise, but it's now final, and firms that start

acting on it now will be ahead of everyone scrambling closer to the CPE deadlines.

This has been building for a while. ICAI set up DAAB a few years ago specifically to deal with accounting and assurance issues in digital environments and given how much of a modern statutory audit already touches IT systems, cloud infrastructure and automated processes, a dedicated set of IS audit standards was only a matter of time.

What Does it Involve?

The compendium runs to **eleven standards**, numbered ISAS 110 through 610, covering the full arc of an IS audit. ISAS 110, 210 and 220 deal with scoping and planning - defining the nature of the assurance being given and understanding how a client's technology maps onto its business objectives. ISAS 310 and 320 govern execution: a structured work programme, professional scepticism, and a detailed set of expectations around what ISAS calls the "**digital artifact lifecycle**" - how electronic evidence gets identified, collected, preserved, analysed and eventually disposed of.

The standards that will matter most on a day-to-day basis are the technical ones in the middle: ISAS 410 on IT general and application controls, ISAS 420 on auditing AI, blockchain and big-data tools, ISAS 430 on Digital Personal Data Protection compliance, and ISAS 440 on cybersecurity audits specifically. ISAS 510 and 610 close things out on reporting and quality control.

Why This Matters Beyond Compliance?

Until now, there was no ICAI standard telling auditors how to actually audit a client's IT environment with any real authority - which is a big part of why IT and cybersecurity consultants ended up picking up so much of that work by default. ISAS gives CA firms a credible basis to offer cybersecurity assurance, DPDP compliance reviews and controls testing as proper standalone engagements, rather

AUDITOR'S LENS

than something loosely bundled into the statutory audit and never quite billed for. For clients, it also means a clearer, more consistent standard to expect from any IS audit work they commission going forward



A few things worth knowing:

ISAS 320 formalises how electronic evidence is expected to be handled - worth checking existing practice against it before a regulator or client asks.

ISAS 420 expects auditors to test whether AI-driven results are reproducible, not just plausible. That's a different skill from what most audit teams currently have.

ISAS 610 requires 20 hours of CPE per year specifically in IS audit subjects, on top of everything else - worth building into training plans well before year-end

What Firms Should be Doing Now?

Firms would do well to map their current audit methodology against the eleven standards and see where the gaps sit - evidence handling and automated-tool testing look like the two weakest points industry-wide. Engagement letters and audit programmes for clients with significant digital infrastructure should be reviewed too, so IS risk is scoped in explicitly rather than assumed to be covered somewhere inside the financial audit.

More detail will follow as ICAI issues further clarifications, but the direction of travel is clear enough to start preparing for now.

THERESA MILEENA N. S

ARTICLED ASSISTANT

Email ID: rojanilin@gmail.com



Options Uncovered: Understanding the Right to Buy or Sell

Financial markets are constantly influenced by changes in interest rates, currency movements, commodity prices, corporate developments and investor sentiment. With such uncertainty, investors and businesses need instruments that can help them manage financial risk.



An option is a type of derivative contract whose value is linked to an underlying asset such as a share, stock market index, commodity or currency. Unlike a conventional purchase or sale, an option gives the buyer a right, but not an obligation, to buy or sell the underlying asset at a predetermined price within or on a specified

date. This unique feature makes options useful not only for investors seeking returns but also for businesses and investors looking to manage risk.

What Exactly is an Option?

At its simplest, an option creates an arrangement between two parties:

- ❖ The option buyer obtains a right.
- ❖ The option seller (writer) assumes an obligation if the buyer exercises that right.
- ❖ The buyer pays a price known as the premium for obtaining this right.

There are two fundamental types of options:

1. Call Option

A Call Option gives the buyer the right, but not the obligation, to buy the underlying asset at a predetermined price.

An investor may purchase a call option when they expect the price of the underlying asset to increase.

2. Put Option

A Put Option gives the buyer the right, but not the obligation, to sell the underlying asset at a predetermined price.

An investor may purchase a put option when they expect the price of the underlying asset to decline or when they want protection against a fall in the value of an asset they already hold

Understanding the Key Terms

Underlying Asset:

The asset, index or reference variable on which the option derives its value.

Strike Price

The predetermined price at which the buyer can exercise the option

Premium

The amount paid by the option buyer to the option seller for obtaining the right.

Expiry Date

The date on which the option contract expires

Option Buyer

The party who purchases the option and obtains the right.

Option Seller/Writer

The party who receives the premium and assumes the corresponding obligation

A Simple Example of a Call Option

Suppose the shares of ABC Ltd. are currently trading at ₹1,000.

An investor believes that the price may rise significantly over the next two months. Instead of purchasing the shares directly, the investor purchases a “**call option**” with:

Strike Price: ₹1,050, Premium: ₹30 per share, Expiry: Two months

If, at expiry, the share price rises to ₹1,150, the investor can exercise the option and buy at ₹1,050.

The intrinsic benefit is: $₹1,150 - ₹1,050 = ₹100$

After considering the premium of ₹30, the net gain is: $₹100 - ₹30 = ₹70$ per share

However, if the share price remains below ₹1,050 at expiry, the investor may choose not to exercise the option. In that situation, the maximum loss to the buyer is generally limited to the premium paid, i.e., ₹30 per share.

This illustrates one of the important characteristics of buying options: the potential loss for the buyer can be limited to the premium paid, while the potential gain may be substantially higher depending on the option and underlying asset.

Call vs Put: The Basic Difference

Particulars	Call Option	Put Option
Right	Right to buy	Right to sell
Generally used when	Expecting price to rise	Expecting price to fall
Buyer pays	Premium	Premium
Buyer has	Right, not obligation	Right, not obligation

Options as a Risk-Management Tool

Options are not merely instruments for speculation. One of their most important applications is hedging.

Consider an investor who owns shares worth ₹10 lakh but is concerned that the market may decline in the near future. The investor could consider an

appropriate “**put option**” strategy to provide protection against a fall in value.

Similarly, businesses exposed to movements in currencies, commodities or interest rates may use options as part of their

broader risk-management strategy.

The objective is not necessarily to eliminate risk completely, but to limit the impact of unfavourable movements while retaining some benefit from favourable movements.

Options and Speculation

Options are also used by market participants who seek to benefit from anticipated price movements.

Because options generally require the buyer to pay a premium rather than the full value of the underlying asset,

they can provide exposure to a larger underlying position for a relatively smaller initial outlay. However, this should not be mistaken for low risk. The value of an option can be affected by several factors, including: price of the underlying asset, strike

price, time remaining until expiry, Volatility, Interest rates, Market expectations. Consequently, an option can lose significant value even when the investor's broad market direction is correct.

The Importance of Time: Time Value of an Option

One of the fascinating characteristics of options is that time itself has value. An option with several months remaining before expiry may be worth more than an otherwise identical option with only a few days

remaining, because there is more time for the underlying asset to move favourably.

As the expiry date approaches, the option's time value generally declines. This phenomenon is

commonly referred to as time decay.

Therefore, an option buyer is not only taking a view on the direction of the market but is also effectively taking a view on timing.

Key Takeaway

Options are powerful financial instruments because they combine flexibility, risk management and market exposure within a single contractual framework.

For a prudent market participant, the key question should not simply be:

“How much can I make?”

but rather:

“What risk am I taking, how much can I lose, and why am I entering this contract?”

Used with proper understanding and disciplined risk management, options can be an effective tool for navigating uncertainty in modern financial markets.

An option does not remove uncertainty—it provides a structured way to manage it.

ASWATHY R NAIR

ASSURANCE AND CONSULTING STAFF- 2

Email ID: nairaswathy1997@gmail.com



When AI Goes Wrong, Who Answers for It?

Artificial Intelligence has moved rapidly from a futuristic concept to an everyday business tool. Businesses now use AI to draft emails and contracts, analyse data, create content, assist customers, screen applications and make recommendations.

But when an AI system produces a harmful or inaccurate result, an important legal question arises:

Who is Responsible?

Imagine an AI system providing incorrect financial information, generating defamatory content, making an unfair hiring recommendation, exposing confidential information, or producing material that infringes intellectual property rights.

AI itself does not generally have legal personality. It cannot independently enter into contracts, pay compensation or appear before a court as a legal defendant. As a result, the law must usually look at the people and organisations involved in developing, supplying, deploying and using the system.

The real question, therefore, is not simply whether AI made a mistake, but **who was responsible for the way the AI was designed, deployed and used.**



1. Can AI Be Held Legally Responsible?

At present, AI systems are generally not treated as independent legal persons capable of being sued or punished in the same way as individuals or companies.

Depending on the circumstances, potential responsibility may therefore fall on different parties:

- **The developer**, if the system was negligently designed or contained serious defects.

- **The service provider**, if adequate safeguards, warnings or security measures were not provided.
- **The business using the AI**, if it relied on the system without appropriate controls or supervision.
- **An employee**, where the system was knowingly or

negligently misused.

- **Other parties**, such as technology suppliers or integrators, depending on their role.

This makes the allocation of responsibility an important part of managing AI-related legal risk.

DOMAIN SPECIFIC CORNER

2. When AI Gives Wrong Advice

One of the most significant risks arises when businesses rely on AI for professional or important decisions.

For example, suppose a company asks an AI system to analyse a contract. The system incorrectly states that the company has no liability under a particular clause. The company relies on the answer, signs the contract

and later suffers financial loss.

The company cannot necessarily avoid responsibility by saying, **“The AI told us so.”**

AI-generated information should generally be treated as assistance rather than an automatic substitute for professional judgment. This

is particularly important in areas such as:

Legal advice | Tax | Finance | Healthcare | Recruitment | Compliance

The greater the potential consequences of a decision, the more important it becomes to verify AI-generated information and maintain appropriate human review.

3. AI and Data Privacy

AI systems often process significant amounts of information, creating another major area of legal risk: **data privacy and confidentiality**.

Consider an employee uploading a customer's personal information, financial records or confidential business documents into an online AI tool.

The business must then consider questions such as:

- Was the employee authorised to share the information?
- What happens to the information after it is uploaded?
- How is the information stored and processed?
- Is it used for any additional purposes?

- What security measures are in place?

In India, the **Digital Personal Data Protection Act, 2023** provides an important framework for the processing of digital personal data. Businesses using AI should therefore pay careful attention to their obligations concerning personal data, security safeguards and lawful processing.

A practical rule is simple:

“Do not put confidential or personal information into an AI system unless you understand how that information will be handled.”

4. Who Owns AI-Generated Content?

AI can produce articles, images, designs, software code, presentations, marketing material, music and other creative outputs. This creates difficult questions concerning intellectual property.

Who owns AI-generated content?

The answer may depend on factors such as the applicable law, the extent of human involvement, the terms of the AI service and the nature of

the material used to generate the output.

There is also a separate concern: **copyright infringement**.

An AI-generated image, text or design may resemble

DOMAIN SPECIFIC CORNER

existing protected material. Businesses should therefore avoid if everything produced by AI is automatically free from intellectual-property risk.

Before commercially using significant AI-generated

material, businesses should consider:

- Who owns the output?
- Were third-party materials involved?

- Does the AI provider impose contractual restrictions?
- Could the output infringe another person's intellectual-property rights?

5. AI in Recruitment and Employment

AI is increasingly being used to screen CVs, rank candidates and assist with recruitment. However, automated systems can reproduce patterns contained in the data on which they were trained.

For example, historical recruitment data may contain discriminatory patterns. An AI system trained on that

data could unintentionally reproduce those patterns when evaluating new applicants.

An employer may therefore face legal and reputational risks even if the discriminatory outcome was produced by an algorithm.

Saying “**the computer made the decision**” does not

necessarily remove the employer's responsibility.

Businesses using AI in employment decisions should consider fairness, transparency, human review and proper documentation. Decisions affecting a person's employment or livelihood require particular care.

6. Contracts and AI Liability

AI-related risks should also be addressed when businesses enter into agreements with technology providers.

Contracts should, where appropriate, clarify:

- Who bears responsibility for losses caused by the AI system?

- What happens if confidential information is compromised?
- Who owns AI-generated content?
- What security measures must the provider maintain?
- What are the data-breach notification obligations?

- Are there limitations or exclusions of liability?
- Can customer data be used to train or improve the AI model?

Clear contractual terms can help businesses understand where responsibility lies before a dispute arises.

A Practical Example

Consider a company that uses an AI chatbot to communicate with customers.

A customer asks whether a product qualifies for a refund. The chatbot incorrectly states that the customer is entitled to a full refund, even though the company's actual policy does not allow it.

The customer relies on the statement and demands the refund.

Who is responsible?

There is no universal answer. The legal position may depend on factors such as:

DOMAIN SPECIFIC CORNER

How the chatbot was designed → Who controlled it → Whether the company approved its use → What information the chatbot was given → Whether its responses were monitored → Whether the customer suffered legally recognisable loss

7. What Should Businesses Do?

Businesses do not necessarily need to avoid AI. Instead, they should create sensible safeguards around its use.

A Practical AI Legal-Risk Checklist :

1. Create an AI-use policy

Clearly identify what employees may and may not use AI for.

2. Protect confidential information

Do not upload sensitive business or personal information without appropriate authorisation and safeguards.

3. Keep humans involved in important decisions

Legal, financial, employment and compliance decisions should receive appropriate human review.

4. Verify AI-generated information

AI can produce convincing but inaccurate information. Important facts should be independently checked.

5. Review AI contracts

Understand the provider's terms concerning data, confidentiality, intellectual property, security and liability.

6. Maintain records

For significant decisions, document how AI was used, what review was undertaken and who ultimately approved the decision.

Conclusion

AI can increase efficiency, improve decision-making and transform the way businesses operate. But using AI does not make legal responsibility disappear. When something goes wrong, the relevant questions will often be:

Who designed the system? Who supplied it? Who deployed it? Who controlled it? Who relied on its output? And what safeguards were in place?

As AI becomes more deeply integrated into business and society, these questions will become increasingly important. The goal should not be to fear AI, but to **use it responsibly**—with appropriate human oversight, data protection, contractual safeguards and awareness of the legal risks involved.

AI may generate the answer, recommendation or content—but businesses and individuals must still take responsibility for how that technology is used.

DOMAIN SPECIFIC CORNER

ASWATHI MURALEEDHARAN

HR MANAGER, ASSURANCE AND CONSULTING
STAFF-1

Email ID: aswathyvinu1998@gmail.com



Tax Planning vs Tax Evasion.

Tax is an important financial obligation for every taxpayer. While taxpayers naturally seek to reduce their tax burden, it is essential to understand the difference between legitimate tax planning and illegal tax evasion. The distinction lies primarily in whether the taxpayer follows the law and acts transparently.

What is Tax Planning?

Tax planning refers to the lawful arrangement of financial affairs to minimise tax liability while complying with applicable tax laws.

A taxpayer may make use of deductions, exemptions, rebates and other benefits specifically provided under the law. For example, choosing an appropriate tax regime, making eligible investments or claiming legitimate business expenses can form part of tax planning.

- ❖ Effective tax planning should be based on:
- ❖ Compliance with applicable tax laws
- ❖ Proper documentation
- ❖ Genuine transactions
- ❖ Appropriate use of available deductions and exemptions



- ❖ Long-term financial objectives
- ❖ Thus, tax planning is not about avoiding tax illegally; it is about organising financial affairs efficiently within the framework of the law.

What is Tax Evasion?

Tax evasion is the deliberate and illegal attempt to reduce or avoid tax by concealing income, misrepresenting facts or providing false information to the tax authorities.

Examples may include:

- | | |
|--|--|
| <ul style="list-style-type: none"> ❖ Concealing taxable income ❖ Recording fictitious expenses ❖ Suppressing sales or receipts ❖ Maintaining false books of accounts | <ul style="list-style-type: none"> ❖ Claiming deductions that are not legally available ❖ Providing false information in tax returns |
|--|--|

Tax evasion can result in interest, penalties, prosecution and other legal consequences.

DOMAIN SPECIFIC CORNER

The Role of Chartered Accountants

Chartered Accountants play an important role in helping taxpayers understand and comply with tax laws. Professional advice should focus on legitimate tax planning rather than aggressive or unlawful methods of reducing tax liability.

A Chartered Accountant must maintain professional ethics, exercise due diligence and ensure that financial and tax information presented to authorities is accurate and properly supported.

Conclusion

Tax planning and tax evasion may appear similar because both can result in a lower tax liability, but their legal and ethical foundations are completely different.

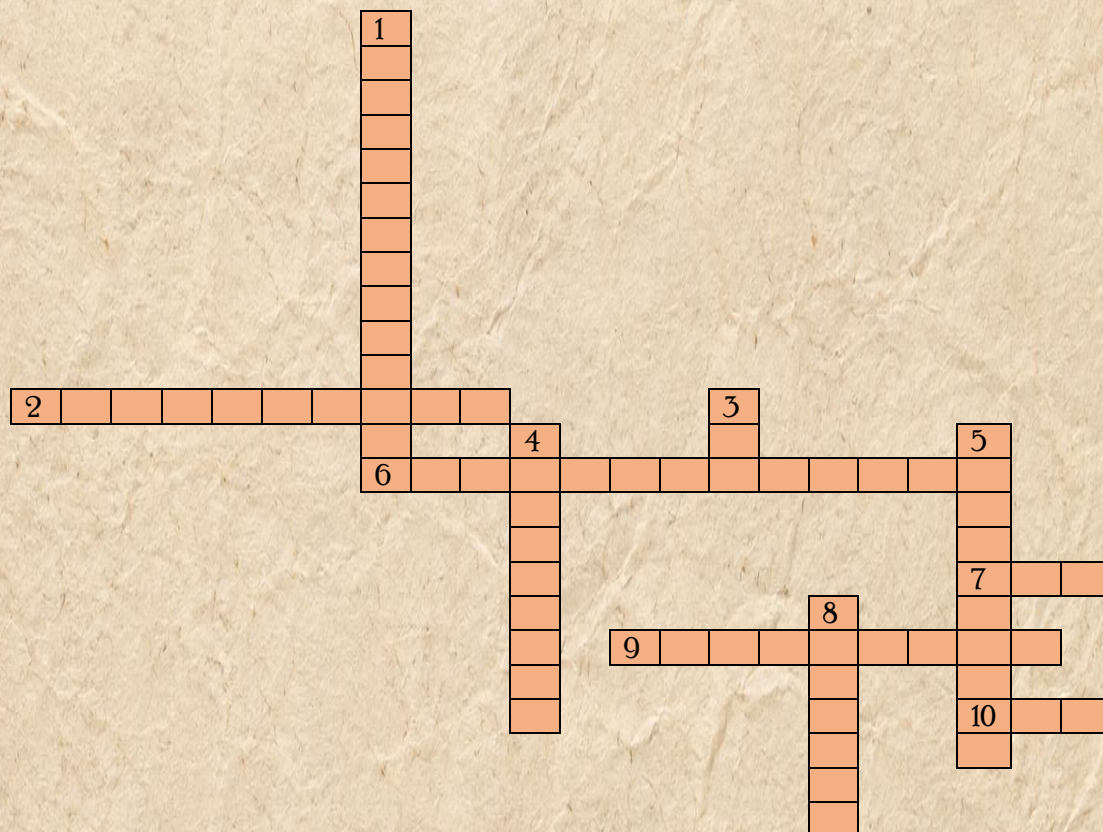
“Tax planning works within the law; tax evasion works against the law.”

A responsible taxpayer should aim not merely to minimise tax but to achieve tax efficiency through lawful, transparent and well-documented financial planning. In the long run, compliance and ethical conduct provide a stronger foundation than short-term gains achieved through unlawful practices.

CROSSWORD PUZZLE

CROSSWORD

✂ This month's crossword features key terms from Income Tax, GST, Corporate Law, and FEMA. Test your knowledge and see how many you can solve!



ACROSS

2. The constitutional document that defines a company's scope and relationship with the outside world.
6. Income remaining after considering eligible deductions for determining tax liability.
7. Tax deducted by the payer at the prescribed rate from specified payments.
9. GST charged by a registered person on taxable outward supplies.
10. Unique identification number allotted to a company by the Ministry of Corporate Affairs.

DOWN

1. Credit available under GST for eligible tax paid on inward supplies, set off against output tax.
3. Investment by a person resident outside India in an Indian business with a lasting interest.
4. Statement filed with the Income-tax Department declaring income and relevant tax particulars.
5. Transfer of money from one country to another, subject to applicable foreign-exchange rules.
8. Independent professional appointed to examine a company's financial statements.

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

Across: Agent, ISD, 320, Add, COUNT, 182

Down: Questioning, Costing, Current, Infinite

MEMORY BOX

TEACHER'S DAY CELEBRATION



BIRTHDAY CELEBRATION



इपवेटरइव

SEPTEMBER 2026 ISSUE – 9

e Newsletter from NITIN N & CO. Chartered Accountants

Thank you for reading

Scan here



For more