VOLUME 1 | ISSUE 21 | January 2026

THE WORLDONOMICS TIMES

CMA CA Sandeep Kumar, Editor-in-Chief, The Worldonomics Times, honoured with the " Yes, I can Achiever Award" from Shri Sunil Shashti Ji(Son of Shri Lal Bahadur Shashtri Ji) in the presence of Shri Surendra Sharma Ji, Dr. Ashutosh Karnataka Ji(Former CMD of GAIL India), CMA R C Gupta Ji, along with the Approach Team.


THE
WORLDONOMICS
TIMES
www.worldonomics.in


THE
WORLDONOMICS
TIMES
Innovation, Wealth, and Global Shifts. Focus on the future of business, tech, and changing cultural landscapes.
www.worldonomics.in


THE
WORLDONOMICS
TIMES
CAREER COUNSELLING PROGRAM BY CMA SANDEEP KUMAR AND TEAM THE WORLDONOMICS TIMES
www.worldonomics.in


THE
WORLDONOMICS
TIMES
THE RANCHI PRESS CLUB
Dr. Ravindra Kumar Rai, President (Working), Jharkhand State BJP and Shri Samir Oraon, National President Tribe Wings BJP at Viksit Bharat Youth Summit 2025, Ranchi
www.worldonomics.in

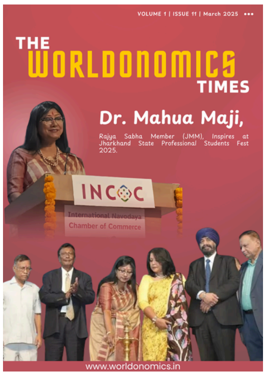

THE
WORLDONOMICS
TIMES
Shri Arun Singh Ji, General Secretary BJP as Chief Guest, CMA Sanjay Jindal Ji, Director Finance EIL, CA Atul Gupta Ji, Former President, ICAI, CMA Madhuri Kashyap Former President, INCOC at Professional Youth For Viksit Bharat - Delhi
SIP
www.worldonomics.in


THE
WORLDONOMICS
TIMES
Decoding Cost Audit: Rules, Relevance, and Reporting
Is Selling Old Gold Taxable? An Expert Analysis
AI as an Assistant: Understanding the Power of Generative vs. Predictive Models
Rethinking Credit Assessment: Why SMEs are Stuck Behind the Credit Wall
www.worldonomics.in


THE
WORLDONOMICS
TIMES
Innovation Ignition: Fueling Economic Growth
Overview of Risk Analysis in Mutual Funds
Shri Joshit Ranjan Sikidar
Director Finance
Solar Energy Corporation of India Limited
Prosperity's Promise: Economic Growth Starts with Human Development
www.worldonomics.in

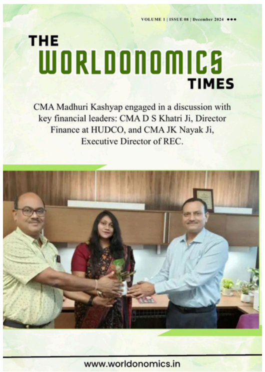

THE
WORLDONOMICS
TIMES
The Future of Gold: Technology, Tokenization and the Green Economy
Cybersecurity Costs and Risk Accounting for CMAs
Green Hydrogen (GH2): Potential, Prospects & Challenges in India
Artificial Intelligence: Ethical Considerations and Future Prospects
CS Dhananjay Shukla
President
The Institute of Company Secretaries of India
Auditing in the Digital Age: Transforming Assurance and Compliance

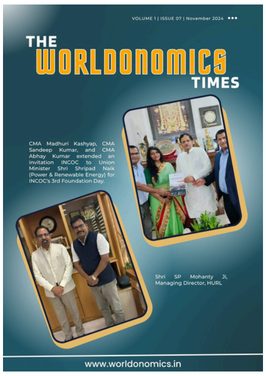

THE
WORLDONOMICS
TIMES
Representatives held a meeting with CMA Rajesh Dwivedi, Director Finance at BHEL, to discuss finance-related matters.
www.worldonomics.in

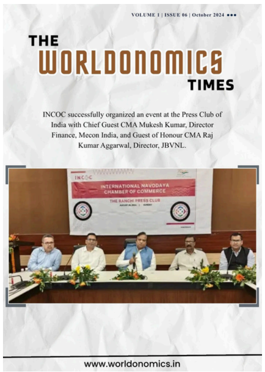

THE
WORLDONOMICS
TIMES
Dr. Mahua Maji,
INCOC
www.worldonomics.in


THE
WORLDONOMICS
TIMES
CMA BK Shokey Ji, Former Director Finance, NBCC and CMA Geeta Sharma Ji, Former Director Finance, HLL
CA Anju Thakur Ji, Executive Director, HUDCO
www.worldonomics.in


THE
WORLDONOMICS
TIMES
INCOC hosted an event at the Constitution Club of India, Delhi, featuring CMA Sanjay Jindal, Director Finance, Engineers India Limited, as the Chief Guest and CA Bimal Jain as the Speaker, with the guidance of their Mentor Shri BK Shabharwal Ji.
www.worldonomics.in


THE
WORLDONOMICS
TIMES
CMA Madhuri Kashyap engaged in a discussion with key financial leaders: CMA D S Khatri Ji, Director Finance at HUDCO, and CMA JK Nayak Ji, Executive Director of REC.
www.worldonomics.in


THE
WORLDONOMICS
TIMES
www.worldonomics.in


THE
WORLDONOMICS
TIMES
INCOC successfully organized an event at the Press Club of India with Chief Guest CMA Mukesh Kumar, Director Finance, Mecon India, and Guest of Honour CMA Raj Kumar Aggarwal, Director, JBVNL.
www.worldonomics.in


THE
WORLDONOMICS
TIMES
www.worldonomics.in


THE
WORLDONOMICS
TIMES
INNOVATION IGNITION
FUELING ECONOMIC GROWTH
PROSPERITY'S PROMISE
Shri Anuj Gupta
Head - Commodity and Currency Market
HDFC Securities
UNITY IN PROSPERITY
GLOBAL COLLABORATION FOR GROWTH
SPENDING POWER ON THE RISE


THE
WORLDONOMICS
TIMES
BUILDING A BRIGHTER FUTURE TOGETHER
LEADING THE WAY
Shri Jay Prakash Gupta
Founder- Dhan
Co - Founder Raise Fintech Ventures
POLITICAL AND ECONOMIC STABILITY
MARKET AND ECONOMY


THE
WORLDONOMICS
TIMES
NURTURING GROWTH
EMPOWERING INDIVIDUALS
POWERING CHANGE
INSPIRING ACTION
DRIVING CHANGE
SHAPING A BRIGHTER FUTURE
SHRI NAVEEN MATHUR
www.worldonomics.in


THE
WORLDONOMICS
TIMES
ACTIONABLE IMPACT
EMPOWERING CHANGE
BUILDING FUTURES
LEAD WITH IMPACT
www.incoc.in


INCOC
International Navodaya
Chamber of Commerce


THE RANCHI PRESS CLUB
AUGUST 24, 2025 |
Chief Guest:
Dr. Ravindra Kumar Rai
State President (Working)
BJP Jharkhand

THE WORLDONOMICS TIMES

PUBLISHED BY

INTERNATIONAL NAVODAYA CHAMBER OF COMMERCE

Established in 2021
Volume 1 | Issue 21 | January 2026 | Knowledge Box

The Worldonomics Times
30/26A, Street No. 9
Vishwas Nagar, Delhi 110032
Tel: +91 11 69268366

Email Us
For Circulation, sponsorship and inquiry
info@incoc.in

Website
www.worldonomics.in
MRP: ₹ 190
Delhi Legal Jurisdiction

From the Editor's Desk

Dear Esteemed Readers,

Empowering the Global MSME Community

At the International Navodaya Chamber of Commerce (INCOC), we see a world of boundless opportunity for those willing to adapt. Our collective mission is to empower entrepreneurs to move beyond "gut-feel" decisions toward actionable, impact-driven results. By embracing the spirit of "Jai Jawan, Jai Kisan, Jai Vigyan," we honor our professional roots while championing the science and technology—such as Artificial Intelligence—that will define our future.

A Commitment to Shared Growth

I encourage you to use the insights within these pages—from GST updates to credit assessment strategies—to not only grow your revenue but to build resilient, sustainable organizations. Thank you for your continued trust and readership as we work together to lead with impact throughout 2026.

As we welcome the dawn of January 2026, I find myself reflecting on the incredible journey of the global MSME community. This year marks a pivotal chapter in our collective history—one where the boundaries between traditional business wisdom and cutting-edge digital innovation are blurring more rapidly than ever before. At The Worldonomics Times, our mission has always been to provide a bridge between these two worlds, and this issue is a testament to that commitment.

On a deeply personal note, I am humbled to share that I was recently honored with the "Yes, I Can Achiever Award" for Innovation in Learning. Receiving this recognition from Shri Sunil Shastri Ji, the son of the legendary Shri Lal Bahadur Shastri Ji, in the presence of stalwarts like Dr. Ashutosh Karnataka, was a moment of immense pride—not just for me, but for the entire International Navodaya Chamber of Commerce (INCOC) family. This award serves as a powerful reminder that "Innovation in Learning" is not just a phrase; it is the lifeblood of survival in the 21st century.

In this edition, we tackle the "Digital Age" head-on. We explore how artificial intelligence is moving from the realm of science fiction into the practical toolkit of the everyday entrepreneur. From automating customer service to precision-based inventory forecasting, AI is no longer a luxury—it is a necessity for those who wish to "Lead with Impact." However, with great technological advancement comes great responsibility. This is why I have personally authored a featured piece in this issue regarding Cybersecurity Basics. As we migrate our operations to the cloud, protecting our data from common threats must be our top priority. A single security breach can undo years of hard-earned trust, and we must fortify our digital borders with the same diligence we use to manage our physical assets.

Furthermore, we continue to provide critical updates on GST regulations, credit assessment strategies, and investment avenues like tax-saving bonds. Our goal is to ensure that while you look toward the future, your foundations remain compliant and financially sound.

As the National President of INCOC, I see a world of boundless opportunity for those willing to adapt. The transition from "gut-feel" management to data-driven strategy is the hallmark of the modern leader. I encourage you to use the insights within these pages to not only grow your revenue but to build resilient, sustainable, and secure organizations.

Let us embrace 2026 with a spirit of "Jai Jawan, Jai Kisan, Jai Vigyan"—honoring our roots while championing the science and technology that will define our future.

Thank you for your continued trust and readership.

CA CMA Sandeep Kumar
Editor-in-Chief
The Worldonomics Times
Founder & President
International Navodaya Chamber of Commerce

INTERNATIONAL NAVODAYA CHAMBER OF COMMERCE

DELHI HEAD OFFICE

Alankrit Society, A-31, Plot A1,
Vishwas Nagar, New Delhi-110032

info@incoc.in

+91 8506060306 / 8506060506

JHARKHAND STATE OFFICE

Shop No. 8, Balaji Corporate Park,
North Upar Bazar, Ranchi - 834001

jharkhand@incoc.in

+91 9257157192 / 9934012264


CA CMA SANDEEP KUMAR
National President


CA SANGAM AGGARWAL
National Vice President


CMA MANOJ KUMAR SINGH
State Head - Jharkhand


RAJ KISHORE SAHU
Member State Team

www.incoc.in

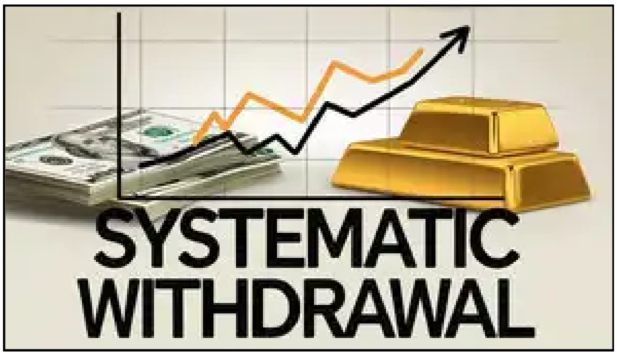
TABLE OF CONTENTS   PAGE NUMBER

Systematic Withdrawal Plan: A Sustainable Income Strategy for Long-Term Retirement Planning

Retirement marks the onset of a new chapter in life, offering individuals the opportunity to prioritise their own interests and well-being. During this period, many can finally dedicate time to hobbies, enjoy leisure activities, and experience a sense of tranquillity. However, achieving this freedom relies heavily on continued income, which is essential once traditional salaried employment ends.

Historically, retirees depended on sources of income such as pensions, fixed deposits, rental income, and interest from savings to finance their golden years. However, various economic factors have changed this landscape. With declining interest rates, rising inflation on essential goods, increasing medical expenses, and longer life expectancies, relying solely on a substantial retirement corpus is no longer sufficient. It's crucial to convert these savings into a stable, inflation-adjusted monthly income to maintain financial security in retirement.

In this scenario, the Systematic Withdrawal Plan (SWP) offered by mutual funds becomes one of the most effective and flexible tools for retirees in the post-retirement era.



In this detailed article, we will understand:

- What SWP is and how it works
- Why SWP is better than traditional income sources
- A practical example with the SWP amount
- How long the corpus may last
- Why the SWP amount or corpus must sometimes be revised
- Strategies to improve SWP sustainability

1. What is SWP (Systematic with-drawal Plan)?

An SWP allows an investor to withdraw a fixed amount regularly (monthly, quarterly, or annually) from a mutual fund. The remaining money continues to be invested, growing through market returns based on the scheme you have opted for.

In simple terms:

- You invest a lump sum amount in a mutual fund scheme
- You receive regular income at each interval, say, monthly
- Your remaining money grows based on the fund's performance

It makes SWP a perfect tool for retirees who need a substitute for a monthly salary.

SWP = Regular Income + Growth + Liquidity + Flexibility

In an annuity product, your money is locked in permanently, and you receive a fixed amount at a specified date, either monthly, quarterly, half-yearly, or annually, which you opt for when buying the annuity product.

Whereas in SWP, you have the freedom to withdraw any amount at any time, flexibility to change or stop SWP at any time, and complete control over your capital. In SWP, return is not fixed; it is based on market conditions. However, in the long term, it helps you beat inflation due to decent returns.

This combination of income and accessibility makes SWP one of the most powerful retirement solutions available in India.

2. Why SWP is Superior to Traditional Income Tools?

SWPs (Systematic Withdrawal Plans) are preferable to Fixed Deposits (FDs) because the income generated from mutual funds—such as conservative hybrid funds, aggressive hybrid funds, and large-cap funds—tends to be significantly higher than that from FDs. Additionally, mutual funds are more tax-efficient.

This higher income allows retirees to maintain their current lifestyle and effectively combat inflation over the long term. In contrast, the interest on FDs is fixed at the time the FD is opened, without any opportunity for adjustment.

Moreover, the interest earned on FDs is taxed on an accrual basis. For example, if you have a Fixed Deposit of ₹ 1,000,000 at an interest rate of 7% for three years, it will mature after three years. However, you will need to pay income tax on the interest earned each year. This means that you will incur a tax liability of ₹ 70,000 for the first year, based on your income tax slab rate.

On the other hand, with a Systematic Withdrawal Plan, you only pay capital gains tax on the amount withdrawn, depending on the scheme you choose, rather than on the entire investment. This makes SWPs a more flexible and tax-efficient option compared to Fixed Deposits.

Investing in a SWP (Systematic Withdrawal Plan) can often deliver better returns than rental income. Typically, the net yield from rental properties ranges between 3% and 4% of the initial capital invested.

This yield can be volatile and is often subject to market fluctuations. Additionally, property ownership requires ongoing maintenance and management costs each year, which can further impact overall profitability.

When comparing investment options, the Systematic Withdrawal Plan (SWP) offers advantages over traditional Annuity Plans. Generally, the interest rates on Annuities are lower than those on Fixed Deposits (FDs). Additionally, while FDs may not always keep pace with inflation, SWPs offer greater flexibility than Annuities, where your funds are often locked in for extended periods.

Understanding these differences, you can make better financial decisions for your retirement corpus.

3. Benefit of SWP:

1. Inflation-Adjusted Income: Imagine a steady flow of income that not only supports your lifestyle but also keeps pace with the rising cost of living. This feature ensures that your purchasing power remains intact, allowing you to confidently manage your expenses over time.

2. Capital Appreciation: Visualize your investments blossoming like a well-tended garden, growing in value as market conditions change. This potential for capital appreciation transforms your initial Investment into a more substantial asset, enhancing your overall financial wealth.

3. Tax-Efficient Withdrawals: Think of withdrawals designed to minimize your tax obligations. This strategic approach enables you to optimize your returns, allowing you to retain more of your earnings for reinvestment or personal use rather than paying taxes on them.

4. Market-Linked Growth: Envision your investments dynamically connected to the pulse of the market. This feature allows you to tap into the potential of market growth, ensuring your portfolio can flourish alongside economic advancements and trends.

5. Easy Liquidity: Picture having the freedom to access your funds with ease, whenever you need them. This liquidity offers you the flexibility to navigate life's financial demands without the stress of locked-in investments, empowering you to make timely decisions.

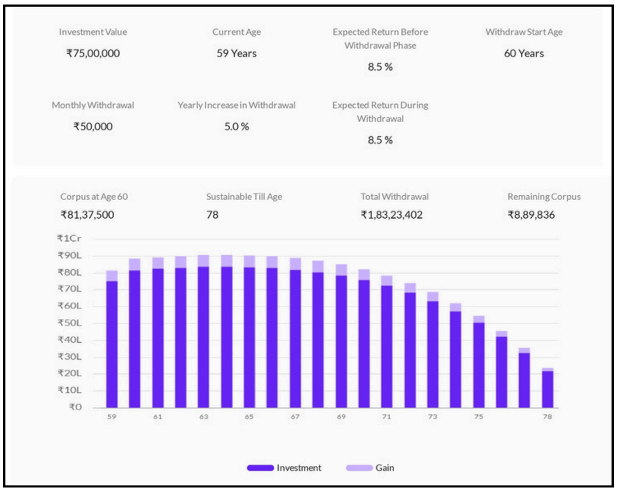
This balance of stability, growth, and flexibility makes SWP the preferred choice for long-term retirement planning.

4. Understanding the Example

Let us take a constructive approach by examining the details through a practical example based on realistic assumptions.

- **Initial Investment: ₹75,00,000**
- **Current Age: 59 years**
- **Withdraw Start Age: 60 years**
- **Monthly Withdrawal: ₹50,000**
- **Annual Withdrawal: ₹6,00,000**
- **Expected Return: 8.5% per year**
- **Inflation: 5% increase in SWP every year**

The annual withdrawal amount is ₹600,000 (₹ 50000 × 12 months), which is 8% per annum on the amount invested (₹ 75,00,000).



The investment strategy is categorised as moderately aggressive, with an expected inflation rate of 5% and a projected return of 8.5%. This approach typically suggests a balanced opportunity for growth while acknowledging potential risks. To further clarify the associated risk levels, the risk matrix is outlined as follows:

- 4% = very safe
- 5–6% = sustainable
- 7–8% = moderately aggressive
- 9%+ = risky

Here, 8% withdrawal + 5% inflation adjustment means the withdrawal amount will rise to:

- At the age of 64: ~₹7.29 lakh
- At the age of 69: ~₹9.30 lakh
- At the age of 74: ~₹11.87 lakh
- At the age of 78: ~₹14.43 lakh

Given the 8.5% return rate, withdrawals will start to outpace investment growth relatively quickly. As a result, the overall corpus is expected to decrease gradually over time. A detailed analysis is presented in Table No. 1.

Table no-1

Age	Withdrawl		Year End Corpus
	Monthly	Yearly	
59			₹ 81,37,500
60	₹ 50,000	₹ 6,00,000	₹ 82,29,188
61	₹ 52,500	₹ 6,30,000	₹ 82,98,668
62	₹ 55,125	₹ 6,61,500	₹ 83,42,555
63	₹ 57,881	₹ 6,94,572	₹ 83,57,097
64	₹ 60,775	₹ 7,29,300	₹ 83,38,147
65	₹ 63,814	₹ 7,65,768	₹ 82,81,121
66	₹ 67,005	₹ 8,04,060	₹ 81,80,958
67	₹ 70,355	₹ 8,44,260	₹ 82,32,080
68	₹ 73,873	₹ 8,86,476	₹ 78,28,333
69	₹ 77,567	₹ 9,30,804	₹ 75,62,944
70	₹ 81,445	₹ 9,77,340	₹ 72,28,458
71	₹ 85,517	₹ 10,26,204	₹ 68,16,673
72	₹ 89,793	₹ 10,77,516	₹ 63,18,577
73	₹ 94,283	₹ 11,31,396	₹ 57,24,266
74	₹ 98,997	₹ 11,87,964	₹ 50,22,870
75	₹ 1,03,947	₹ 12,47,364	₹ 42,02,457
76	₹ 1,09,144	₹ 13,09,728	₹ 32,49,941
77	₹ 1,14,601	₹ 13,75,212	₹ 31,50,975
78	₹ 1,20,331	₹ 14,43,972	₹ 8,89,836

Since returns are only 8.5%, the withdrawals begin to exceed growth soon. This means the corpus will decline gradually over time.

As the 19th year(at the age of 78) draws to a close, the principal amount will be almost entirely depleted. By the time you reach the 20th year(at the age of 79), the remaining balance will stand at ₹8.89 lakhs. It shows that a moderately aggressive withdrawal should be reconsidered, and you should plan a sustainable withdrawal rate of 5-6% for your monthly SWP.

To sum up, the analysis indicates that the Systematic Withdrawal Plan (SWP) can remain viable for approximately 17 to 19 years. However, the initial corpus is expected to decline significantly after about 12 to 14 years. This decline is compounded by the fact that withdrawals tend to outpace portfolio returns, ultimately rendering the SWP unsustainable.

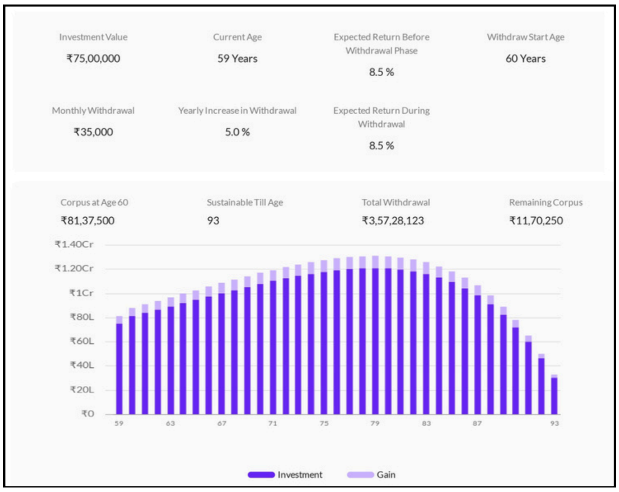
Conclusion

A Systematic Withdrawal Plan is one of the most effective ways to generate stable, tax-efficient, inflation-adjusted income during retirement. However, its sustainability depends on maintaining the right balance between:

- Investment amount
- Monthly Withdrawal
- Expected return
- Inflation

In the given example of a ₹75 lakh investment with a monthly withdrawal of ₹ 50,000, the SWP can provide reliable income for nearly two decades but will eventually face pressure from rising inflation.

Regular reviews, strategic adjustments, and thorough planning are vital components of successful financial management. When approached effectively, a systematic withdrawal plan (SWP) can be an invaluable strategy for achieving long-term financial independence. This allows retirees to enjoy their lives without the constant concern of monthly income fluctuations.



If a retiree opts for a Systematic Withdrawal Plan (SWP) that withdraws ₹ 35,000 per month and provides a sustainable annual return of around 5.50% on the total Investment, they could potentially maintain these withdrawals until age 93. This scenario is illustrated in **Graph 2 above**, which shows the long-term viability of such a withdrawal strategy.

The concept of systematic withdrawal plans (SWP) can differ significantly from person to person, depending on individual needs and lifestyles. It is essential to begin proactive planning at an early stage. By focusing on goal-based investing, you can build a robust retirement corpus and take full advantage of compounding. Your Systematic Withdrawal Plan (SWP) will meet your financial needs throughout your life, and later on, your family will be able to use the remaining funds.

Disclaimer:

The information contained in this document is for general purposes only and should not be considered investment advice. It is compiled from reliable sources, including publicly available data from various websites, newspapers, and internally developed data. The views expressed are opinions and should not be considered guidelines, recommendations, or professional advice.

CMA (Dr.) R K Mohapatra

CMA (Dr.) R K Mohapatra is a Certified Retirement Advisor & Financial Consultant, an Editorial Board Member of "The Worldonomics Times," and an "Eminent Author" awardee. He has 34 years of experience in finance and accounting, including cash and wealth management, financial and retirement planning, and tax planning.

Analysis of Notifications & Circulars - December 2025

Income Tax, GST, Central Excise, Custom Duty, DGFT, SEBI, MCA, IBBI, RBI
(Click the Link for Notification/ Circular as issued)

A. Income Tax

Cancer Institute' (W.I.A), Chennai notified under section 35(1)(ii) for Scientific Research: The notification notifies 'Cancer Institute' (W.I.A), Chennai for 'Scientific Research' under the category of 'University, college or other institution' for the purposes section 35(1)(ii) of the Income-tax Act, read with rules 5C and 5E of the Income-tax Rules. This section allows for deduction equal to one and half times while computing taxes for expenses relating to scientific research.

(Link: Income Tax Notification 175/2025 Dated 30/12/2025)

Indian Institute of Science Education and Research, Pune notified under section 35(1)(ii) for Scientific Research: The notification notifies 'Indian Institute of Science Education and Research', Pune for 'Scientific Research' under the category of 'University, college or other institution' for the purposes section 35(1)(ii) of the Income-tax Act, read with rules 5C and 5E of the Income-tax Rules. This section allows for deduction equal to one and half times while computing taxes for expenses relating to scientific research.

(Link: Income Tax Notification 174/2025 Dated 29/12/2025)

The Christian Medical College Vellore Association, Vellore, Tamil Nadu notified under section 35(1)(ii) for Scientific Research: The notification notifies 'The Christian Medical College Vellore Association', Vellore, Tamil Nadu for 'Scientific Research' under the category of 'University, college or other institution' for the purposes section 35(1)(ii) of the Income-tax Act, read with rules 5C and 5E of the Income-tax Rules. This section allows for deduction equal to one and half times while computing taxes for expenses relating to scientific research.

(Link: Income Tax Notification 173/2025 Dated 29/12/2025)

Exemptions to Punjab Urban Planning And Development Authority: Punjab Urban Planning And Development Authority, an authority constituted under the Punjab Regional and Town Planning and Development Act, 1995, has been notified under section 10(46A) for exemption on its income, provided the authority continues to operate for specified purpose under section 10(46A)(a) of Act.

(Link: Income Tax Notification 172/2025 Dated 15/12/2025)

Exemptions to New Okhla Industrial Development Authority (NOIDA): New Okhla Industrial Development Authority, an authority constituted by the State Government of Uttar Pradesh, has been notified under section 10(46) for exemption on its income arising from amount received as Grants from state government, disposal of properties, rent, fees, tolls, charges under UPIADA and interest on bank deposits.

(Link: Income Tax Notification 171/2025 Dated 15/12/2025)

Appellate Authority for Search and Survey Assessments: The notification reallocate appellate jurisdiction among specified Commissioners of Income-tax (Appeals) for search, requisition, and survey- related cases. It authorises designated appellate authorities across multiple locations to exercise powers over appeals arising from assessments completed pursuant to searches under section 132, requisitions under section 132A, or surveys under section 133A, including cases where additions are based on seized or impounded material and related penalty orders.

(Link: Income Tax Notification 170/2025 Dated 15/12/2025)

Exemptions to Tamil Nadu Pollution Control Board: Tamil Nadu Pollution Control Board, a board constituted under the Water (Prevention and Control of Pollution) Act 1974 and the Air (Prevention and Control of Pollution) Act, 1981 by the State Government of Tamil Nadu, has been notified under section 10(46A) for exemption on its income, provided the authority continues to operate for specified purpose under section 10(46A)(a) of Act.

(Link: Income Tax Notification 169/2025 Dated 04/12/2025)

Exemptions to Ajmer Development Authority: Ajmer Development Authority, an authority constituted under the Ajmer Development Authority Act 2013, has been notified under section 10(46A) for exemption on its income, provided the authority continues to operate for specified purpose under section 10(46A)(a) of Act.

(Link: Income Tax Notification 168/2025 Dated 04/12/2025)

Exemptions to Jalandhar Development Authority: Jalandhar Development Authority, an authority constituted under the Punjab Regional and Town Planning and Development Act 1995, has been notified under section 10(46A) for exemption on its income, provided the authority continues to operate for specified purpose under section 10(46A)(a) of Act.

(Link: Income Tax Notification 167/2025 Dated 04/12/2025)

Deduction under section 80G allowed for Shree Balakrishna Lalji Temple Renovation: Shree Balakrishna Lalji & other deities temple located in Bhuvneshwar, Mumbai, and managed by Mata Mandir Trust, has been notified, as a place of historic importance and public worship renowned across Maharashtra and Gujarat under Section 80G(2)(b) of Income Tax Act. It enables donors to claim deductions for contributions made specifically towards the renovation or repair of the temple. The approval is strictly restricted to donations up to Rs 50 crore and remains valid until the sanctioned amount is fully collected or until 31st March 2030, whichever occurs earlier.

(Link: Income Tax Notification 166/2025 Dated 02/12/2025)

B. GST

Valuation of supply of specified goods on the basis of declared Retail Sale Price (RSP): The notification insert a new Rule 31D in the CGST Rules, which provides that, notwithstanding any other provisions, the value of supply of notified goods shall be deemed to be the retail sale price declared on such goods, reduced by the amount of applicable tax.

(Link: CGST Notification 20/2025 Dated 31/12/2025)

Retail Sale Price based valuation under GST for Pan Masala, Tobacco and Cigarette Products w.e.f. 1st Feb 2026: The notification provide for valuation of supply of certain specified goods on the basis of declared Retail Sale Price (RSP) under the CGST Act. The specified goods covered under the notification include pan masala, unmanufactured tobacco (other than tobacco leaves), cigars, cheroots, cigarillos and cigarettes, other manufactured tobacco and tobacco substitutes, as well as products containing tobacco or nicotine substitutes intended for inhalation without combustion.

The retail sale price has been defined as the maximum price declared on the package, inclusive of all taxes, duties, cess or surcharges.

(Link: CGST Notification 19/2025 Dated 31/12/2025)

GST Rate on Biris at 9%, Tobacco & Pan Masala at 20% effective 1st Feb 2026: Pan Masala, Cigarettes, Tobacco and similar products will attract a 20% CGST (Total 40% including SGST 20%), while Biris will be taxed at 9% GST (Total 18% including SGST 9%), as per the notification. The Schedule VII, i.e. items with 14% CGST rate and all related entries have been deleted. Similar notifications have been issued under IGST and UTGST.

(Link: CGST Notification (Rate) 19/2025 Dated 31/12/2025, IGST Notification (Rate) 19/2025 Dated 31/12/2025, UTGST Notification (Rate) 19/2025 Dated 31/12/2025)

Compensation Cess at NIL Rate on Pan Masala and Tobacco effective 1st Feb 2026: The notification has notified the reduction of Goods and Services Tax (Compensation to States) Cess to 'Nil' on specified pan masala and tobacco products.

(Link: Compensation Cess Notification (Rate) 03/2025 Dated 31/12/2025)

GSTAT Benches allotted to ensure Nationwide GST Appellate Functioning: The Government of India, has approved the allotment of benches to appointed members of the Goods and Services Tax Appellate Tribunal (GSTAT). The order specifies postings for three categories, i.e. Technical Members (Centre), Technical Members (State), and Judicial Members, across multiple locations nationwide, including metropolitan centres and regional benches. This administrative action formalises bench composition and postings, enabling GSTAT to function effectively and provide structured appellate adjudication under the GST regime across India.

(Link: FinMin Office Order 03/2025 Dated 26/12/2025)

Staggered GST Appeal filing withdrawn after Portal Review: GSTAT has revoked its earlier order dated 24th September 2025 that had mandated staggered filing of appeals under Section 112 of the CGST Act. The earlier arrangement required appeals arising from orders under Sections 107 and 108 to be filed in phases, based on portal capacity constraints. Upon reassessing the technical readiness and capabilities of the GSTAT appeal portal, it has been decided to discontinue the staggered filing mechanism.

(Link: GSTAT Order 315/2025 Dated 26/12/2025)

Advisory & FAQ on Electronic Credit Reversal and Re-claimed Statement & RCM Liability/ITC Statement: The advisory clarifies the operation and upcoming validations for the Electronic Credit Reversal and Re-claimed Statement (ITC Reclaim Ledger) and the RCM Liability/ITC Statement (RCM Ledger) to ensure accurate reporting and prevent excess ITC claims. The ITC Reclaim Ledger tracks temporary ITC reversals in Table 4(B)(2) and subsequent reclaims in Tables 4(A) (5) and 4(D)(1) of GSTR-3B. The RCM Ledger, tracks RCM liability in Table 3.1(d) and corresponding ITC in Tables 4(A)(2)/(3). While warnings currently appear, the portal will soon block GSTR-3B filing where reclaims or RCM ITC exceed available balances. Taxpayers with negative balances must mandatorily reverse excess ITC or pay additional RCM liability before filing.

(Link: GSTN Advisory Dated 29/12/2025)

Advisory, Consolidated FAQs on GSTR - 9/9C for FY 2024-25: GSTN has released consolidated FAQs, consolidating clarifications issued in October and December 2025. The FAQs explain system enablement of annual returns, auto-population logic from GSTR-1, 1A, IFF, 2B and 3B, and detailed reporting of Input Tax Credit across multiple scenarios such as claim, reversal and reclaim spanning different financial years. The key clarifications include the introduction of Table 6A1 for separating ITC of preceding years, refined treatment of reclaimed ITC under Rules 37/37A, revised logic for Tables 8A, 8B, 8C and 8D to avoid mismatches, and new reporting for import IGST claimed in subsequent years through Table 8H1. The FAQs also clarify treatment of RCM liabilities, non-GST purchases, HSN reporting support through downloadable utilities, removal of the 65% concessional rate option.

(Link: GSTN Advisory Dated 17/12/2025, Consolidated FAQs)

Advisory on reporting values in Table 3.2 of GSTR-3B: The advisory clarifies regarding reporting values in Table 3.2 of Form GSTR-3B, relating to inter-state supplies made to unregistered persons, composition taxpayers, and UIN holders. From November tax period onward, the values auto-populated in Table 3.2 based on GSTR-1, GSTR-1A ond IFF filings will become non-editable, and taxpayers must file GSTR-3B using only the system generated figures. If corrections are needed, amendments must be made through Form GSTR-1A for the same tax period, which will automatically update Table 3.2 in real time. Form GSTR-1A can be submitted any time after GSTR-1 and up to the moment of filing GSTR-3B.

(Link: GSTN Advisory Dated 05/12/2025)

Advisory, Auto Suspension of GST Registration due to Non-Furnishing of Bank Account Details: Taxpayers, other than those registered under TCS, TDS, or on a suo motu basis, must provide their bank account details within 30 days of registration or before filing GSTR-1 or IFF, whichever occurs earlier. If these details are not submitted within the prescribed time, the system will automatically suspend the taxpayer's GST registration. Once the details are furnished, the system will automatically drop cancellation proceedings. Alternatively, taxpayers may manually initiate the dropping process if it does not occur the same day.

(Link: GSTN Advisory Dated 05/12/2025)

Advisory, FAQs on Annual Return GSTR -9/9C for FY 2024-25: Additional list of Frequently Asked Question (FAQs) along with the response has been issued intended to assist the Taxpayer in better understanding and reporting of values in various Tables of GSTR-9/9C. Ineligible ITC availed for FY 2023-24 but claimed or reversed in FY 2024-25 must be reported in Table 6A1 of GSTR-9, while reversals pertaining to FY 2023-24 need not be included elsewhere. Table 12B of GSTR-9C may show mismatches if prior year ITC is booked in the current year, and explanations can be provided in Table 13. ITC received for FY 2023-24 but claimed in FY 2024-25 is to be reported in Table 6A1, with unreconciled differences explained. Non-GST purchases are not reported in GSTR-9, and Table 4G1 applies only to e-commerce operators under section 9(5) of the CGST Act.

(Link: GSTN Advisory Dated 04/12/2025) (FAQs)

SC, GST Exemption allowed as Hostel Use qualifies as Residential Dwelling: Case of State of Karnataka vs Taghar Vasudeva Ambrish, SC Judgement Dated 4th December 2025.

The apex court ruled that renting a residential property for use as a long-term hostel/PG for students/professionals qualifies for GST exemption, even if leased to a company, as the core 'residential dwelling' use and the ultimate occupants 'residential purpose' (eating, sleeping) fulfils the exemption criteria (Entry 13). It overrules revenue attempt to deny it based on commercial operation or a direct lessee's status. The ruling clarifies that exemption hinges on the nature of the property and end-use for residence.

(Link: SC Judgement Dated 4/12/2025)

HC, Cross-LoC Barter Trade with PoK is Intra-State Supply: Case of New Gee Enn & Sons vs Union of India, HC J&K Judgement Dated 27th November 2025. The court ruled that trade between J&K and PoK (Pakistan occupied Kashmir) is Intra-State supply, under GST Act, since PoK Is part of J&K Territory. Traders engaged in cross-LoC trade should treat supplies as intra-state under GST, and respond accordingly if they receive notices.

(Link: HC J&K Judgement Dated 27/11/2025)

HC, Attachment Order Lapses after one-year limit under GST Law: Case of Devansh Wire and Cables Private Limited vs Union of India, HC Delhi Judgement Dated 11th November 2025. The court noted that under Section 83(2) of the CGST Act, any order issued under Section 83(1) ceases to operate after one year, and therefore the impugned attachment order was no longer operative. Accordingly, it directed that the concerned bank should not restrict operations of the petitioner bank account based on the impugned order, and the Sub-Registrar should not block transfer of the petitioner immovable property on the same basis.

(Link: HC Delhi Judgement Dated 11/11/2025)

AAR, Aerated Beverages in Restaurants taxable as Composite Service: Case of Summit Hotels & Resorts Pvt Ltd, AAR West Bengal Ruling Dated 10th December 2025. AAR ruled that aerated beverages supplied in a hotel restaurant, whether alone or with meals, are not standalone goods but form part of a composite supply of restaurant services. Accordingly, GST is levied at the rate applicable to restaurant services for specified premises.

(Link: AAR West Bengal Ruling Dated 10/12/2025)

AAR, Clarifications on Homoeopathic Medicines HSN Classification and GST Rates: Case of Sett Dey and Co Homoeo Lab, AAR West Bengal Ruling Dated 10th December 2025. AAR clarified that the term "medicament" encompasses all forms of medicines and remedies used for therapeutic or prophylactic purposes. Products manufactured in accordance with authoritative pharmacopoeia formulae and sold under the names specified therein fall within the scope of Schedule I entries 233 and 234. The ruling confirmed that for all applicable categories, the GST rate 5% is applicable.

(Link: AAR West Bengal Ruling Dated 10/12/2025)

AAR, Essential Hospital support services held GST-Exempt for meeting "Pure Service" Criteria: Case of Ex Servicemen Settlement Society, AAR West Bengal Ruling Dated 10th December 2025. AAR ruled that the security and scavenging services being supplied by the applicant to Government of West Bengal hospitals qualify as pure services related to functions entrusted under Articles 243G and 243W. Accordingly, such services fall under Serial No. 3 of Notification 12/2017 and are exempt from GST.

(Link: AAR West Bengal Ruling Dated 10/12/2025)

AAR, GST Exemption limited to Manpower-Based Municipal Services: Case of Shubhabrata Chowdhury, AAR West Bengal Ruling Dated 10th December 2025. AAR ruled that manpower-related services qualify as pure services under Entry 3. For all remaining maintenance-related services, exemption under Entry 3A applies only if the goods component does not exceed 25%. If it exceeds 25%, the services are taxable as per Notification 11/2017.

(Link: AAR West Bengal Ruling Dated 10/12/2025)

AAR, GST Exemption on Road Transport for E-Commerce Deliveries, treated as GTA Service: Case of Flipkart India Private Limited, AAR West Bengal Ruling Dated 9th December 2025. The applicant stated that under the proposed model, after customers purchase goods on the ECO portal, sellers shall deliver the goods to a Source Mother Hub. The applicant then collect goods from that hub and transports them to customers delivery addresses, potentially through multiple transit hubs. The applicant stated that it would issue a single consignment note for each shipment from the Source Mother Hub to the delivery address, regardless of changes in vehicle or transit points. The applicant also assumes responsibility for the goods until delivery, including liabilities for damage and arranging transit insurance. AAR ruled that the new logistics model qualify as Goods Transport Agency (GTA) services and are exempt from GST when supplied to unregistered end customers under Serial No. 21A of Notification 12/2017 (Rate).

(Link: AAR West Bengal Ruling Dated 09/12/2025)

AAR, GST exemption for Household Water Data Collection Services: Case of Chhanda Bhattacharya, AAR West Bengal Ruling Dated 9th December 2025.

AAR held that the collection of household data for Functional Household Tap Connections (FHTCs) using mobile applications or other instruments constitutes pure services provided to the State Government in relation to functions entrusted to Panchayats and Municipalities. As such, these services fall within Entry 3 of Notification 12/2017 (Rate) and are exempt from GST.

(Link: AAR West Bengal Ruling Dated 09/12/2025)

AAR, GST Exemption for Transfer of Business as Going Concern: Case of Horizon Edge Technologies Pvt Ltd, AAR West Bengal Ruling Dated 9th December 2025. AAR held that the transfer of assets and liabilities from Horizen to the applicant qualifies as a service by way of transfer of a going concern and is exempt under Entry 2 of Notification 12/2017 (Rate). The invoices and supplies issued in furtherance of, or as an extension of, original work orders will retain identical taxability. Other work orders executed post-transfer, related to government functions, qualify as exempt pure services.

(Link: AAR West Bengal Ruling Dated 09/12/2025)

AAR, Tea and Premix Bundles classified as Mixed Supply: Case of Jivraj Tea International Pvt Ltd, AAR Gujarat Ruling Dated 4th December 2025.AAR ruled that in all cases i.e. whether black tea, CTC leaf tea, green tea variants, herbal tea, pyramid tea bags, or flavoured tea, the bundling of instant premix tea sachets was held to qualify as mixed supply. Accordingly, all such supplies would be taxed at 5% rate of GST.

(Link: AAR Gujarat Ruling Dated 04/12/2025)

AAR, GST @ 18% applicable on Waste-Processing Machinery supplied to Municipality: Case of Vishalsinh Mahendrasinh Atodariya, AAR Gujarat Ruling Dated 24th November 2025. AAR ruled that supply of goods to the Anand Municipality Corporation attract GST, and that all items listed in the applicant query were liable to 18% rate of GST.

(Link: AAR Gujarat Ruling Dated 24/11/2025)

AAR, ITC not allowed on IGST paid via Pre-Consultation Letter/TR-6 Challan: Case of Hansben Jayantibhai Patel, AAR Gujarat Ruling Dated 24th November 2025. AAR ruled that Input Tax Credit cannot be availed on the additional IGST paid pursuant to a pre-notice consultation letter issued under Section 28(1) of the Customs Act. It clarified that neither the pre-consultation letter nor TR-6 challan qualifies as a prescribed document for claiming ITC.

(Link: AAR Gujarat Ruling Dated 24/11/2025)

AAR, GST @ 5% applicable on Transport of Empty Containers by Rail: Case of Hansi Petro Chemical & Shipping Limited, AAR Gujarat Ruling Dated 24th November 2025. AAR held that, in the case of empty containers, no goods are transported in the container, rather the container itself is the good being transported. It concluded that empty containers qualify as "goods," and their transportation by rail attracts the GST @ 5% under Entry 9(i), subject to the prescribed condition.

(Link: AAR Gujarat Ruling Dated 24/11/2025)

AAR, Bio-Diesel Fuel eligible for ITC under Forward Charge for GTA Services: Case of Amitkumar Maheshbhai Gulwani, AAR Gujarat Ruling Dated 24th November 2025. The applicant proposes to purchase renewable hydrocarbon bio-diesel (Mileage Diesel), taxable at 18%, to be used as fuel in their trucks for providing outward GTA services. The AAR held that the applicant may continue paying GST under forward charge, and availing full ITC, including on bio-diesel, subject to the prescribed conditions.

(Link: AAR Gujarat Ruling Dated 24/11/2025)

AAR, Imitation Zari Yarn classified under 56050020, GST @ 5% Applicable: Case of Sai Ram Jari Industries, AAR Gujarat Ruling Dated 24th November 2025. AAR ruled that the supply of imitation zari thread or yarn manufactured from metallised polyester or plastic film containing aluminium metal and commonly used in sarees and dress materials in lieu of real gold or silver zari, attracts 5% GST.

(Link: AAR Gujarat Ruling Dated 24/11/2025)

AAR, PVC Raincoats classified under Plastics, GST rate at 18%: Case of Pradeepkuar Gaurishankar Trivedi, AAR Gujarat Ruling Dated 24th November 2025. AAR ruled that PVC raincoats attract 18% GST under Entry 111 of Schedule III of Notification No. 1/2017 (Rate), and not the 5% rate applicable to apparel.

(Link: AAR Gujarat Ruling Dated 24/11/2025)

AAR, GST applies on Lease Property used for Commercial Accommodation: Case of Goldie Ashokbhai Shah, AAR Gujarat Ruling Dated 19th November 2025. AAR ruled that the service of renting of Residential building by the applicant to the lessee, an unregistered person, to use it as the residential accommodation for the students and the working professional is subject to GST.

(Link: AAR Gujarat Ruling Dated 19/11/2025)

AAR, GST Payable only on Worker Canteen Deductions, not Employee Deductions: Case of Zydus Hospira Oncology Private Limited, AAR Gujarat Ruling Dated 19th November 2025. AAR ruled held that recovery of subsidized canteen charges from full-time employees does not amount to a supply under Section 7 of the CGST Act, as it is covered by Schedule III and clarified by Circular 172/04/2022.

Therefore, No GST is payable on the portion recovered from employees. However, recovery of subsidized canteen charges from contractual workers amounts to a taxable supply. GST is payable on the portion recovered from contractual workers.

(Link: AAR Gujarat Ruling Dated 19/11/2025)

AAR, GST Liability arises due to Non-Monetary Gifts/ Perquisites/ Tour packages because TDS is Deducted: Case of TVL Kartik, AAR Tamil Nadu Ruling Dated 17th November 2025. AAR ruled that non-monetary benefits such as gifts, perquisites, and tour packages received by a dealer from a manufacturer amount to consideration for "support services" and are exigible to Goods and Service Tax (GST).

(Link: AAR Tamil Nadu Ruling Dated 17/11/2025)

AAR, GST Exemption allowed on Godown Rent due to storage of Agricultural Produce: Case of Leena Modern Rice Mill, AAR Tamil Nadu Ruling Dated 17th November 2025. AAR ruled that the rent received for a godown used exclusively for the storage of paddy is exempt from Goods and Services Tax (GST).

(Link: AAR Tamil Nadu Ruling Dated 17/11/2025)

AAR, Quick Lime (90%) and Hydrated Lime (85-95%) attract 5% GST: Case of Kaycee Industrial Chemicals Private Ltd, AAR Tamil Nadu Ruling Dated 17th November 2025. AAR ruled that Quick Lime and Hydrated Lime containing impurities and having a purity below 98% were classifiable under HSN 2522 as industrial lime and attract a Goods and Services Tax (GST) of 5%.

(Link: AAR Tamil Nadu Ruling Dated 17/11/2025)

AAR, GST Not applicable on Escrow Transfers of Freight Payments: Case of B2B Trucks Private Limited, AAR Tamil Nadu Ruling Dated 17th November 2025. The company acts as a digital facilitator and uses a specific bank account to temporarily hold funds transferred from shippers to be paid to carriers. They do not take responsibility for the physical movement of goods. AAR clarified that the amounts held in this current/escrow account, which are purely for the purpose of forwarding payment to the actual carriers, do not constitute "supply" or "consideration" for B2B Trucks Private Limited's service and are therefore not subject to GST.

(Link: AAR Tamil Nadu Ruling Dated 17/11/2025)

C. Central Excise

Monthly Excise Duty rates notified for Chewing Tobacco, Jarda and Gutkha Manufactured Using Packing Machines: As per the notification, Chewing Tobacco and Jarda Scented Tobacco, and Gutka will attract additional excise duty. It will be in addition to GST as applicable. It applies to chewing tobacco (including filter khaini), jarda scented tobacco, and gutkha. The levy is applicable where these notified goods are manufactured with the aid of packing machines and packed in pouches bearing a declared retail sale price (RSP). The duty structure is based on two key parameters, i.e. Retail Sale Price (RSP) per pouch, and Speed of the packing machine, measured in pouches per minute.

(Link: Central Excise Notification 04/2025 (T) Dated 31/12/2025)

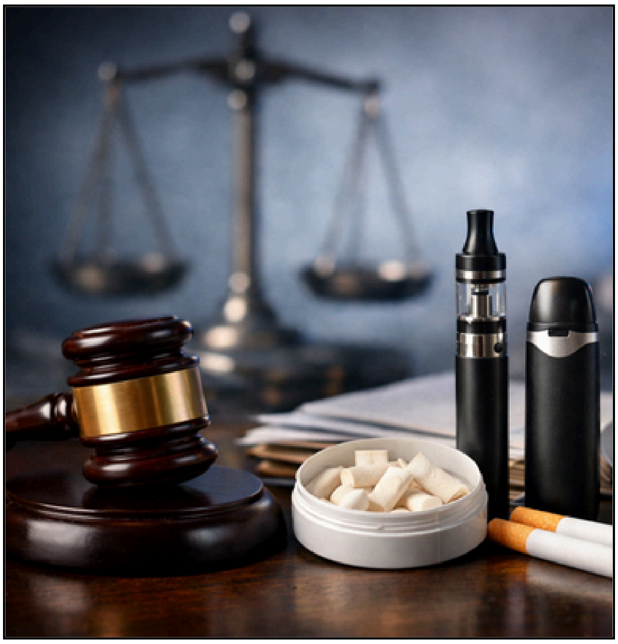
Revision of Central Excise Duty Rates on Tobacco and Related Products: As per the notification, Cigarettes, Hukka and other such specified goods will attract additional excise duty. It will be in addition to GST as applicable. Under the new framework, excise duty on unmanufactured tobacco (Heading 2401) has been set at 18%. Cigarettes attract duty based on length and type, with rates ranging from Rs. 2,050 to Rs. 8,500 per thousand, or ad valorem rates such as 21% or Rs 4,170 per thousand, whichever is applicable. Tobacco substitutes, cigarillos, and other smoking products have also been assigned revised ad valorem or specific rates.

(Link: Central Excise Notification 03/2025 (T) Dated 31/12/2025)

Central Excise notification amended to specifically include Gutkha: The earlier excise notification 01/2022 (NT), dated 1st February 2022 related to tobacco products, has been amended to substitute the words 'Pan masala containing tobacco' with 'Gutkha' in the relevant table. It is intended to bring greater clarity and consistency in the excise treatment and regulation of Gutkha.

(Link: Central Excise Notification 06/2025 (NT) Dated 31/12/2025)

Capacity based Excise Rules for Chewing Tobacco, Gutkha and Jarda: CBIC has notified the Chewing Tobacco, Jarda Scented Tobacco and Gutkha Packing Machines (Capacity Determination and Collection of Duty) Rules 2026, which will come into force with effect from 1st February 2026.



It reintroduces a capacity-based levy system under section 3A of the Central Excise Act. Under the new framework, excise duty will be determined based on the number of packing machines installed and their maximum rated production capacity, linked to the retail sale price (RSP) of pouches.

(Link: Central Excise Notification 05/2025 (NT) Dated 31/12/2025)

Centre notifies Chewing Tobacco, Jarda and Gutkha under Section 3A Excise Levy: The notification brings specified tobacco products under the excise duty regime based on packing capacity. As per the notification, chewing tobacco, jarda scented tobacco and gutkha, when manufactured with the aid of packing machines and packed in pouches, will be treated as notified goods under Section 3A of the Central Excise Act. The notification clarifies that chewing tobacco includes filter khaini and defines packing machines comprehensively.

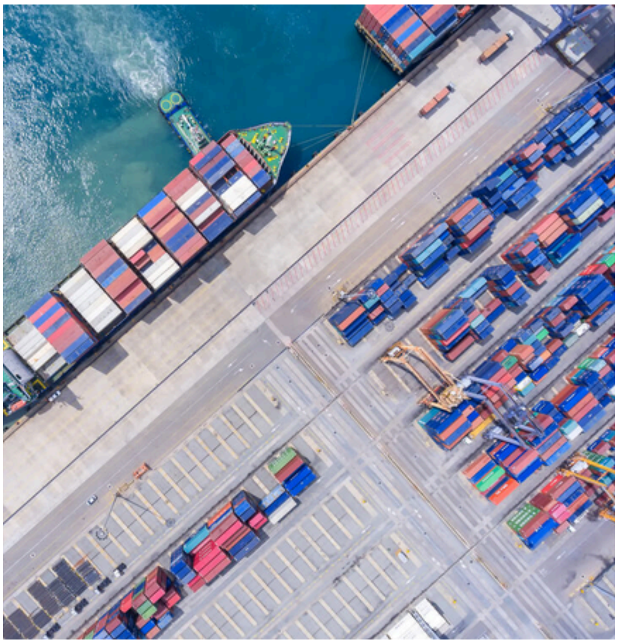
(Link: Central Excise Notification 04/2025 (NT) Dated 31/12/2025)

Central Excise (Amendment) Act, 2025 to come into Force from 1st February 2026: As per the notification, the provisions of Central Excise (Amendment) Act 2025 shall come into force from 1st February 2026. The amendments seek to levy a higher excise duty on tobacco and related products.

(Link: Central Excise Notification 03/2025 (NT) Dated 31/12/2025)

Amendments to Central Excise Act: Central excise duties on many items were repealed with the introduction of GST in 2017, except for some items such as tobacco and tobacco products, liquor, petroleum. The amendments seek to levy a higher excise duty on tobacco and related products once GST compensation cess ends to keep taxes on them at existing level.

(Link: Central Excise Notification Dated 11/12/2025)



D. Custom Duty

Implementation of second tranche of tariff concessions under India-EFTA withIceland: The earlier notification 43/2025 dated 30th September, 2025 has been amended in line with India's commitments under the India–EFTA Trade and Economic Partnership Agreement (TEPA), with Iceland. The Table containing CD rates, AIDC rates and Health Cess rates has been substituted.

(Link: Customs Notification 53/2025 (T) Dated 30/12/2025)

Implementation of second tranche of tariff concessions under India-EFTA with Norway: The earlier notification 42/2025 dated 30th September, 2025 has been amended in line with India's commitments under the India–EFTA Trade and Economic Partnership Agreement (TEPA), with Norway. The Table containing CD rates, AIDC rates and Health Cess rates has been substituted.

(Link: Customs Notification 52/2025 (T) Dated 30/12/2025)

Implementation of second tranche of tariff concessions under India-EFTA with Switzerland: The earlier notification 41/2025 dated 30th September, 2025 has been amended in line with India's commitments under the India–EFTA Trade and Economic Partnership Agreement (TEPA), with Switzerland. The Table containing CD rates, AIDC rates and Health Cess rates has been substituted.

(Link: Customs Notification 51/2025 (T) Dated 30/12/2025)

Implementation of fifth tranche of tariff concessions under India-Australia ECTA: The earlier notification 62/2022 dated 26th December, 2022 has been amended in line with India's commitments under India- Australia Economic Cooperation and Trade agreement (ECTA). The Table containing CD rates, AIDC rates and Health Cess rates has been substituted.

(Link: Customs Notification 50/2025 (T) Dated 30/12/2025)

Fixation of Tariff Value of Edible Oils, Brass Scrap, Areca Nut, Gold and Silver: CBDT notified the Tariff Values of Edible Oils, Brass Scrap, Areca Nut, Gold and Silver, which shall come into force w.e.f. 1st January 2026. The tariff value for crude palm oil is set at USD 1077 per metric ton, while gold and silver have tariff values of USD 1405 per 10 grams and USD 2413 per kilogram, respectively. The tariff value for areca nuts is fixed at USD 7679 per metric ton.

(Link: Customs Notification 80/2025 (NT) Dated 31/12/2025)

Amendments to The Sea Cargo Manifest and Trans-shipment Regulations: The notification pertains to the extension of the filing deadline for the Sea Cargo Manifest and Trans-shipment Regulations till 31st March 2026. The amendment specifically relates to the information required to be submitted in Form-XII Table.

(Link: Customs Notification 79/2025 (NT) Dated 31/12/2025)

Fixation of Tariff Value of Edible Oils, Brass Scrap, Areca Nut, Gold and Silver: CBDT notified the Tariff Values of Edible Oils, Brass Scrap, Areca Nut, Gold and Silver, which shall come into force w.e.f. 31st December 2025. The tariff value for crude palm oil is set at USD 1035 per metric ton, while gold and silver have tariff values of USD 1398 per 10 grams and USD 2406 per kilogram, respectively. The tariff value for areca nuts is fixed at USD 7679 per metric ton.

(Link: Customs Notification 78/2025 (NT) Dated 30/12/2025)

Fixation of Tariff Value of Edible Oils, Brass Scrap, Areca Nut, Gold and Silver: CBDT notified the Tariff Values of Edible Oils, Brass Scrap, Areca Nut, Gold and Silver, which shall come into force w.e.f. 16th December 2025. The tariff value for crude palm oil is set at USD 1035 per metric ton, while gold and silver have tariff values of USD 1398 per 10 grams and USD 2081 per kilogram, respectively. The tariff value for areca nuts is fixed at USD 7679 per metric ton.

(Link: Customs Notification 77/2025 (NT) Dated 15/12/2025)

Fixation of Tariff Value of Edible Oils, Brass Scrap, Areca Nut, Gold and Silver: CBDT notified the Tariff Values of Edible Oils, Brass Scrap, Areca Nut, Gold and Silver, which shall come into force w.e.f. 12th December 2025. The tariff value for crude palm oil is set at USD 1044 per metric ton, while gold and silver have tariff values of USD 1336 per 10 grams and USD 1969 per kilogram, respectively. The tariff value for areca nuts is fixed at USD 7142 per metric ton.

(Link: Customs Notification 76/2025 (NT) Dated 11/12/2025)

Anti-dumping Duty on Low Ash Metallurgical Coke originating in or exported from Australia, China, Columbia, Indonesia, Japan and Russia: Anti-dumping Duty has been imposed on imports of Low Ash Metallurgical Coke originating in or exported from Australia, China, Columbia, Indonesia, Japan and Russia and imported into India. It shall be effective for a period of five years.

(Link: Customs Notification 41/2025 (ADD) Dated 31/12/2025)

Anti-dumping Duty on Hot rolled flat products of alloy or non-alloy steel reduced by amount of Safeguard Duty: The notification amends the Anti-dumping Duty on Hot rolled flat products of alloy or non-alloy steel, originating in or exported from Vietnam and imported into India, imposed vide notification32/2025 (ADD) dated 12th November 2025. It has been amended to provide that, since safeguard duty has been imposed on the subject goods vide Notification 02/2025 (SG) dated 30th December, 2025, the anti-dumping duty equal to the anti-dumping duty mentioned in notification 32/2025, minus the safeguard duty payable, if any, shall be imposed.

(Link: Customs Notification 40/2025 (ADD) Dated 30/12/2025)

Anti- Dumping Duty on PET Resin extended pending Review: The notification 18/2021 (ADD) dated 27th March 2021, has been amended to extend the validity of the existing anti-dumping duty on imports of Polyethylene Terephthalate (PET) resin with intrinsic viscosity of 0.72 dl/g or higher, originating in or exported from China, pending completion of sunset review investigations. The duty will continue to remain in force up to 26th June 2026.

(Link: Customs Notification 39/2025 (ADD) Dated 26/12/2025)

Anti- Dumping Duty extended as Sunset Review continues on '2-Ethyl Hexanol' Import: The notification 17/2021 (ADD) dated 26th March, 2021 has been amended, to extend the applicability of the existing anti-dumping duty on imports of '2-Ethyl Hexanol' pending completion of a sunset review investigation. The subject goods, classifiable under tariff item 2905 16 20, originate in or are exported from the European Union, Indonesia, Korea RP, Malaysia, Taiwan, and the United States of America. The duty shall continue to remain in force up to 26th June 2026.

(Link: Customs Notification 38/2025 (ADD) Dated 25/12/2025)

Anti- Dumping Duty on Calcium Carbonate Filler Masterbatch originating in or exported from Vietnam: Anti-dumping Duty has been imposed on imports of Calcium Carbonate Filler Masterbatch originating in or exported from Vietnam, and imported into India. It shall be effective for a period of five years.

(Link: Customs Notification 37/2025 (ADD) Dated 24/12/2025)

Anti- Dumping Duty on '1,1,1,2 - Tetrafluoroethane or R- 134a' originating in or exported from China: Anti-dumping Duty has been imposed on imports of '1,1,1,2- Tetrafluoroethane or R-134a' originating in or exported from China, and imported into India. It shall be effective for a period of five years.

(Link: Customs Notification 36/2025 (ADD) Dated 24/12/2025)

Anti-dumping Duty on Cold Rolled Non-Oriented Electrical Steel originating in or exported from China: Anti-dumping Duty has been imposed on imports of Cold Rolled Non-Oriented Electrical Steel originating in or exported from China, and imported into India. It shall be effective for a period of five years.

(Link: Customs Notification 35/2025 (ADD) Dated 18/12/2025)

Anti-Dumping Duty on Faced Glass Wool extended: The existing notification 14/2021 (ADD), dated the 18th March, 2021 has been amended to provide that anti-dumping duty on imports of "Faced Glass Wool in Rolls" falling under tariff heading 7019 and originating in or exported from China, shall remain in force up to 17th June 2026.

(Link: Customs Notification 34/2025 (ADD) Dated 15/12/2025)

CVD on Tempered Glass continued to safeguard Local Industry: The countervailing duty (CVD) on imports of Textured Tempered Glass originating in or exported from Malaysia has been extended to prevent injury to the domestic industry. The CVD was originally imposed byh Notification 3/2021 (CVD) dated 9th March 2021. The existing duty will remain in force until 8th June 2026, unless altered earlier.

(Link: Customs Notification 07/2025 (CVD) Dated 07/12/2025)

Safeguard Duty on Non-Alloy and Alloy Steel Flat Products: Safeguard Duty has been imposed on imports of Non-Alloy and Alloy Steel Flat Products, namely (a) Hot Rolled Coils, Sheets and Plates, (b) Hot Rolled Plate Mill Plates, (c) Cold Rolled Coils and Sheets, (d) Metallic Coated Steel Coils and Sheets, whether or not profiled, including Galvanneal, Coated with Zinc or Aluminium-Zinc or Zinc-Aluminium-Magnesium, and (e) Colour Coated Coils and Sheets, whether or not profiled. It shall be effective for a period of three years.

(Link: Customs Notification 02/2025 (SG) Dated 30/12/2025)

Customs orders Video Recording of passenger interactions at Airports: The instruction mandate the use of Body Worn Cameras (BWCs) by uniformed Customs officers engaged in passenger baggage clearance at international airports, particularly at Red Channel counters. A detailed Standard Operating Procedure prescribes how BWCs must be worn, activated, supervised, and handled during passenger interactions. Recordings are to be securely transferred, encrypted, centrally stored under vigilance supervision, and retained for 90 days unless required for investigations or proceedings.

(Link: Customs Instructions 34/2025 Dated 30/12/2025)

Collection of anti-dumping duty on imports of Titanium Dioxide originating in or exported from China: The High Court had quashed Notification No. 12/2025 (ADD) dated 10th May 2025, which had imposed anti-dumping duty on titanium dioxide imported from or originating in China PR. In response, CBIC has directed to immediately stop the collection of this anti-dumping duty. The instruction clarifies that no further anti-dumping duty should be levied on such imports.

(Link: Customs Instruction 33/2025 Dated 05/12/2025)

E. Directorate General of Foreign Trade (DGFT)

Government restricts import of Low Ash Metallurgical Coke for Six Months: The import of Low Ash Metallurgical Coke, having ash content below 18%, including coke fines/coke breeze and ultra-low phosphorous metallurgical coke (with phosphorous content up to 0.030% and size up to 30 mm with 5% size tolerance), falling under ITC (HS) Codes 27040020, 27040030, 27040040 and 27040090, has been placed under the 'Restricted' category. The restriction will be effective from 1st Jan 26 to 30 Jun26.

Imports of metallurgical coke with ash content above 18%, as well as other imports under above codes, are outside scope of this restriction and shall continue to remain 'Free'.

(DGFT Notification 53/2025 Dated 31/12/2025)

Validity of Minimum Export Price on Natural Honey extended till March 2026: DGFT has extended the validity of the Minimum Export Price of US Dollar 1400 FOB per Metric Ton on Natural Honey till 31st March, 2026. Natural Honey, classified under ITC(HS) Code 04090000, continues to remain freely exportable.

(DGFT Notification 52/2025 Dated 31/12/2025)

Allowing Export of 50,000 MT of Organic Sugar per financial year: The notification provide partial relaxation in the export policy for organic sugar by permitting its export up to an annual ceiling of 50,000 metric tonnes per financial year. It modifies the earlier restriction whereby exports were prohibited until further orders.

(DGFT Notification 51/2025 Dated 29/12/2025)

Import Restrictions due to Low-Priced Potassium Clavulanate Imports: The notification amends the import policy for specific chemical and pharmaceutical items under Chapter 29 of ITC. A new Policy Condition No. 08 has been introduced, restricting imports of diluted Potassium Clavulanate, Potassium Clavulanate (KGA), and specified intermediates used in the manufacture of Clavulanic Acid or Potassium Clavulanate when imported below prescribed CIF value thresholds, up to 30th November 2026. However, exemptions are provided for Advance Authorisation holders, Export Oriented Units, and SEZ units, subject to the condition that the imported goods are not diverted to the Domestic Tariff Area.

(DGFT Notification 50/2025 Dated 18/12/2025)

Diamond Imprest Imports exempted from IGST and Compensation Cess: The existing provision granted exemption from various customs duties for imports made under the Diamond Imprest Authorisation, including Basic Customs Duty, Additional Customs Duty, Education Cess, Anti-dumping Duty, Countervailing Duty, Safeguard Duty, and Transition Product Specific Safeguard Duty. The revised paragraph retains these exemptions and further extends the benefit by exempting such imports from the entire Integrated Tax and Compensation Cess leviable under Section 3 of Customs Tariff Act.

(DGFT Notification 49/2025 Dated 09/12/2025)

Procedure for implementation of Import Management System for import of restricted IT Hardware: The circular prescribe the procedure for implementing the Import Management System (IMS) for the import of restricted IT hardware during the calendar year 2026. The imports of laptops, tablets, all-in-one PCs, ultra-small form factor computers, and servers under HSN 8471 are classified as "restricted." Importers are required to apply online through the DGFT portal for import authorisation under the IMS and any authorisation granted will be valid until 31st December, 2026.

(DGFT Policy Circular 08/2025 Dated 17/12/2025)

Amendments in Handbook of Procedures to standardise permissions for EOUs: The Public Notice relates to Chapter 6 of the Handbook of Procedures (HBP) relating to the Export Oriented Units (EOU) Scheme, A new provision, Para 6.41, has been introduced in Chapter 6 of the Handbook of Procedures. Appendix 6N of Appendices and Aayat Niryat Forms (ANFs) has been notified which prescribes standardised formats of letters and permissions issued by Development Commissioners to EOUs.

(DGFT Public Notice 41/2025 Dated 31/12/2025)

SBER Bank added to authorized Gold Import Banks List under HBP: The Public Notice revises the list of banks authorised by the Reserve Bank of India to import only gold for FY 2025-26. The updated list includes Indian Overseas Bank and Union Bank of India for the full period, and additionally includes SBER Bank with a restricted authorisation. SBER Bank is permitted to import gold solely for domestic consumption, with validity from 25th June 2025 until 31st March 2026.

(DGFT Public Notice 40/2025 Dated 19/12/2025)

Procedure for Allocation of Tariff Rate Quota (TRQ) for gold imports under India-UAE CEPA: DGFT has notified the procedure for the first round of allocation of Tariff Rate Quota (TRQ) for gold imports under tariff head 7108 pursuant to the India–UAE CEPA for FY 2025–26. The allocation will be carried out through a competitive e-auction on the MSTC portal, with an initial quota of 30 metric tonnes, extendable by 50% depending on bid response. In compliance with directions of the Delhi High Court, eligibility for this round is restricted to Micro and Small Enterprises to ensure broader and more inclusive participation, with allocation caps of 10 kg and 25 kg respectively.

(DGFT Public Notice 39/2025 Dated 17/12/2025)

Unit of Measurement amended for import items under SION A-290: The Public Notice amends the Unit of Measurement (UOM) under Standard Input Output Norms (SION) A-290 relating to the export product Metformin HCL. It revise the UOM format for two key import items i.e. Dicyanodiamide and DMF, used in the manufacture of Metformin HCL, replacing the earlier 'kg/kg' notation with a simplified 'Kg'. format.

(DGFT Public Notice 37/2025 Dated 11/12/2025)

List of empanelled Pre-Shipment Inspection Agencies (PSIAs) and inclusion of approvals: The public notice incorporates approvals from Inter-Ministerial Committee (IMC), including the enlistment of two new PSIAs i.e. DD International Global and NI- MET Metals Inc. and the approval for 11 existing PSIAs to add instruments such as Handheld Radiation Survey Meters and Spectrometers. All PSIAs must maintain valid calibration certificates, provide bank guarantees, update equipment mapping, and maintain operational offices and bank accounts in India.

(DGFT Public Notice 36/2025 Dated 11/12/2025)

Revision of ANF 7A and Chapter 7 for Deemed Export Benefits: Suppliers and recipients of goods are now required to submit applications in ANF 7A to the jurisdictional Regional Authority (RA) or Development Commissioner of SEZ/EOU, as applicable. Online submission is mandated, eliminating the need for physical copies, and applicants must upload prescribed documents at the time of filing. Claims can only be filed after full payment for the supplied goods.

(DGFT Public Notice 35/2025 Dated 10/12/2025)

Revision of LOP/LOI validity rules to streamline Extension Process: The amendment relates to extensions of the validity period of Letters of Permission/Letters of Intent (LOP/LOI) for units such as EOUs, BTPs, EHTPs, and STPs. Under the revised framework, once a unit commences production, the validity of its LOP/LOI may be extended for up to five years at a time as per Para 6.01(c) of the HBP. Additionally, the initial two-year validity period may be extended by one more year for justified reasons, except where specific restrictions apply, such as for oil refinery projects.

(DGFT Public Notice 34/2025 Dated 01/12/2025)

Ahmedabad Airport permitted for Personal Carriage of Gems & Jewellery: The amendments expand the list of airports permitted for personal carriage of gems and jewellery parcels for both export and import. Under the revised Para 4.87(a), foreign-bound passengers from EOU/SEZ units and DTA firms may now carry export parcels through Ahmedabad Airport in addition to the previously listed airports. Similarly, the amendment to Para 4.88 allows personal carriage of import parcels by Indian importers or foreign nationals into EOU/SEZ units and DTA firms through Ahmedabad Airport.

(DGFT Public Notice 33/2025 Dated 01/12/2025)

Launch of Market Access Support (MAS) under Export Promotion Mission - NIRYAT DISHA: The Market Access Support (MAS) Intervention under the Export Promotion Mission (EPM) - NIRYAT DISHA has been launched, with a view to strengthening India's export market access through structured support for activities such as Buyer-Seller Meets (BSMS), Reverse Buyer-Seller Meets (RBSMS), trade fairs, exhibitions, and related market access initiatives. It is being operationalised on a pilot basis to facilitate early implementation and active stakeholder participation. Implementation shall be undertaken through the Trade Connect ePlatform (https://www.trade.gov.in).

(DGFT Trade Notice 19/2025 Dated 31/12/2025)

F. Securities and Exchange Board of India (SEBI)

Amendments to SEBI Listing Obligations and Disclosure Requirements (LODR) Regulations: The main amendment across the regulations and multiple schedules is a uniform substitution of terminology, replacing references to 'Share Transfer Agent' with 'Registrar to an Issue and Share Transfer Agent'. The changes have been carried out in Regulation 7, Schedules I, II, III, VI, and VII to ensure consistency in language relating to disclosure obligations, compliance requirements, and reporting formats applicable to listed entities.

(Link: SEBI Notification Dated 15/12/2025)

Amendments and consolidation of SEBI Registrars to an Issue and Share Transfer Agents Regulations: The notification consolidate and replace existing framework, establishing a comprehensive regime for registration, governance, and oversight of registrars to issues and share transfer agents.

The regulations mandate compulsory registration with SEBI, prescribe application procedures, fit and proper criteria, infrastructure and governance requirements, and set a minimum net worth of Rs 50 lakh, with an 18-month transition for existing registrants. A robust compliance architecture is introduced, including appointment of compliance officers, internal controls, fraud prevention systems, whistle-blower mechanisms, and dispute resolution processes. SEBI is empowered to conduct inspections, appoint auditors, and initiate disciplinary action for defaults.

(Link: SEBI Notification Dated 15/12/2025)

Amendments to SEBI Infrastructure Investment Trusts (InvIT) Regulations: The amendment revises the definition of family trusts and intermediaries, requiring them to have a net worth exceeding ₹500 crore to be recognised under the relevant clause. It also aligns the definition of 'qualified institutional buyer' with that under the ICDR Regulations. Another update relates to the definition of 'strategic investor', expanding eligibility to institutional investors, specific foreign portfolio investors, and regulated NBFCs across middle, upper, and top layers. Strategic investors must invest at least 5% of the total offer size.

(Link: SEBI Notification Dated 09/12/2025)

Amendments to SEBI Real Estate Investment Trusts (REIT) Regulations: The amendment inserts a new definition of 'institutional investor', expanding it to include qualified institutional buyers, high- net-worth family trusts, and SEBI registered intermediaries with net worth above Rs 500 crore. It also updates the meaning of 'qualified institutional buyer' by aligning it with ICDR Regulations. It revises the definition of 'strategic investor', widening eligibility to include institutional investors, foreign portfolio investors, and RBI registered middle, upper, and top- layer NBFCs, along with other entities as may be notified. Strategic investors must jointly or individually invest at least 5% of the REIT offer size.

(Link: SEBI Notification Dated 09/12/2025)

Amendments to SEBI Intermediaries Regulations: The amendment inserts a new sub-regulation (1) (da), specifying additional grounds on which a person may be deemed "not fit and proper" to act as an intermediary. It covers three key compliance failures i.e. not meeting prescribed minimum net worth or liquid net worth requirements, failing to achieve the mandated minimum revenue from permitted activities, and not transferring specified activities to a separate business unit as required by SEBI.

(Link: SEBI Notification Dated 03/12/2025)

Amendments to SEBI Share Based Employee Benefits and Sweat Equity Regulations: The amendments relates to ESOPs, share-based benefits, and sweat equity issuances mainly focused on valuation standards.

The definition of "valuer" in Regulation 2 has been updated to align fully with Section 247 of the Companies Act, thereby shifting valuation responsibilities from merchant bankers to independent registered valuers. Regulation 34 has been amended to mandate that all new valuations be conducted only by registered valuers.

(Link: SEBI Notification Dated 03/12/2025)

Amendments to SEBI Substantial Acquisition of Shares and Takeovers Regulations: The amendment inserts a new definition of "valuer" aligned with Section 247 of the Companies Act, and replaces the role of acquirers and managers in determining valuation with an "independent registered valuer." It mandates that valuation of shares must now be conducted by independent registered valuers, while providing a nine-month transition period for ongoing valuation assignments initiated before the amendment takes effect.

(Link: SEBI Notification Dated 03/12/2025)

Amendments to SEBI Merchant Bankers Regulations: The amendment include redefining the "principal officer" role, revising application and registration procedures, introducing minimum net worth and liquid net worth requirements for Category I and II merchant bankers, and mandating minimum revenue generation. It prohibits merchant bankers from managing their own issues or issues where key personnel hold significant shares. It also emphasizes ring-fencing net worth, preservation of accounts for eight years, data localization, and compliance officer responsibilities, including reporting non- compliance to SEBI.

(Link: SEBI Notification Dated 03/12/2025)

Amendments to SEBI Substitution of Registered Post with Speed Post Regulations: The amendments replace references to "registered post" or "Registered A.D." with "Speed Post with Registration" or "Speed Post with Registration with Acknowledgment Due," ensuring uniformity in modes of official communication. Specific provisions and schedules across these regulations are updated to require Speed Post-based communication for notices, submissions, and related procedural requirements.

(Link: SEBI Notification Dated 03/12/2025)

Amendments to SEBI Foreign Venture Capital Investors Regulations: The amendments introduce provisions for a new category called SWAGAT-FI (Single Window Automatic and Generalised Access for Trusted Foreign Investor). It exempts such investors from certain sub-regulations, and allows renewal fees to be paid every ten years from the eleventh year of registration. Additionally, the standard investment limits of 66.67% and 33.33% under the principal regulations will not apply to SWAGAT-FIs.

(Link: SEBI Notification Dated 01/12/2025)

Amendments to SEBI Foreign Portfolio Investors Regulations: The amendments introduce the concept of "Single Window Automatic and Generalised Access for Trusted Foreign Investor" (SWAGAT-FI), covering government related investors and public retail funds, subject to conditions specified by SEBI. Registration fees for SWAGAT-FI are now payable in advance for ten-year blocks. Other changes clarify conditions for registration, swap ratios, and compliance exemptions for SWAGAT-FI.

(Link: SEBI Notification Dated 01/12/2025)

Certification mandated for Compliance Officers of Managers of Alternative Investment Funds (AIFs): The Regulations provide that Managers of AIFs are required to appoint a Compliance Officer who meets eligibility criteria specified by SEBI. The circular specifies that such Compliance Officers must obtain certification by passing the NISM Series-III-C: Securities Intermediaries Compliance (Fund) Certification Examination conducted by the National Institute of Securities Market. Trustees, sponsors, or managers must also ensure that compliance with this requirement is expressly reported in the Compliance Test Report.

(Link: SEBI Circular Dated 30/12/2025)

Standardised Affidavit and reduced documentation for Duplicate Certificates: The circular increases the threshold for simplified documentation from Rs 5 lakh to Rs 10 lakh, thereby expanding the scope of cases eligible for a streamlined process. It introduce a standardised Affidavit-cum-Indemnity format, rationalised documentation requirements for securities valued above Rs 10 lakh, and dispensed with notarisation for cases involving securities up to Rs 10,000, where only an undertaking on plain paper is required. For higher-value cases exceeding Rs 10 lakh, additional safeguards such as FIR or equivalent legal documents and newspaper publication requirements were retained.

(Link: SEBI Circular Dated 24/12/2025)

Enhancing the Facility for Basic Services Demat Account (BSDA): SEBI has introduced further reforms to enhance the Basic Services Demat Account (BSDA) framework with the objective of easing investments for investors and simplifying compliance for Depository Participants (DPs). It decided to exclude Zero Coupon Zero Principal (ZCZP) bonds and delisted securities from the valuation threshold used to determine BSDA eligibility, thereby preventing such instruments from disqualifying eligible investors. It also clarifies valuation norms for illiquid and unlisted securities and mandates that DPs reassess BSDA eligibility quarterly. The demat accounts eligible for BSDA must be opened or converted into BSDA by default unless investors provide explicit, authenticated consent to maintain a regular demat account.

(Link: SEBI Circular Dated 24/12/2025)

Zero-Coupon Debt Securities at reduced Rs 10,000 Denomination: SEBI has modified the conditions for issuing debt securities at a reduced denomination of Rs 10,000 under its circular dated 18th December 2025. The issuers may now privately place listed debt securities at a Rs 10,000 face value whether the instrument is interest-bearing or zero-coupon, provided other conditions remain satisfied.

(Link: SEBI Circular Dated 18/12/2025)

Mandating periodic disclosure requirements for Securitised Debt Instruments (SDIs): The circular, in terms of Regulation 11B of the SEBI (Issue and Listing of Securitised Debt Instruments and Security Receipts) Regulations, requires trustees of special purpose distinct entities to submit specified disclosures on a half-yearly basis to SEBI and to the stock exchanges where the SDIs are listed. Separate disclosure formats have been prescribed for SDIs backed by loans, listed debt securities or credit facility exposures, and for SDIs backed by other types of exposures.

(Link: SEBI Circular Dated 16/12/2025)

Strengthening Governance of Market Infrastructure Institutions (MIIs): The circular amends the SECC Regulations and D&P Regulations regarding appointment, roles, and responsibilities of Managing Directors (MDs), Executive Directors (EDs), Chief Technology Officers (CTO), Chief Information Security Officers (CISO), Chief Risk Officers (CRiO), and Compliance Officers (CO). The key provisions include appointment of EDs through open advertisement, reporting structures of EDs to MDs, quarterly performance evaluations, and modified reporting lines for KMPs. Technology audits will be handled by CRiO, who will also attend relevant committee meetings.

(Link: SEBI Circular Dated 12/12/2025)

Deferment of timeline for implementation of Phase III of Nomination Circular: Earlier phases were staggered across June, September, August, and finally 15th December 2025, due to operational challenges faced by AMCs, RTAs, depositories, and market participants. SEBI has now postponed the Phase III timeline to a future date that will be notified separately.

(Link: SEBI Circular Dated 11/12/2025)

Relaxation on geo-tagging requirement in India for NRIs while undertaking KYC: SEBI has modified the Master Circular on KYC to ease the re-KYC process for existing NRI clients. The requirement for clients to be physically located in India during digital re-KYC has been relaxed. Intermediaries must ensure digital verification apps incorporate features such as random action prompts, time-stamping, geo-location verification, and IP address anti-spoofing measures. The GPS coordinates captured must match the country of the client address proof, ensuring authenticity without the need for physical presence in India.

(Link: SEBI Circular Dated 10/12/2025)

Modalities for migration to AI only schemes and relaxations to Large Value Funds for Accredited Investors: The circular permits existing Alternative Investment Funds (AIFs) or schemes to convert to Accredited Investor (AI)-only or Large Value Funds (LVFs) schemes with investor consent, subject to reporting requirements to SEBI and depositories within 15 days of conversion. AI status of an investor at onboarding is retained throughout the scheme tenure. Maximum permissible extension for AI-only schemes is five years, including prior tenure. LVFs are exempted from following the standard placement memorandum template and annual audit requirements without specific investor waivers.

(Link: SEBI Circular Dated 08/12/2025)

Clarification on the Digital Accessibility: The circular mandates that the 'Investors Right to have digital accessibility' will now be incorporated into all relevant Investor Charters. REs must submit their readiness and compliance status for each digital platform by 31st March 2026 to the designated reporting authorities. SEBI has also provided a standard format for reporting and clarified that investors may lodge accessibility-related complaints on SCORES, which REs must resolve to close the complaint. All REs are required to conduct periodic accessibility audits of websites, apps, and portals through certified accessibility professionals.

(Link: SEBI Circular Dated 08/12/2025)

Securities Markets Code introduced in Lok Sabha: The Securities Markets Code 2025, proposes a comprehensive overhaul of India's securities law framework by repealing and consolidating three legacy statutes governing securities regulation, market oversight, and depositories. The Bill seeks to modernise regulation in line with evolving market practices, technological advancements, and the growing scale of capital markets. A key reform is the decriminalisation of minor and procedural defaults, replacing criminal sanctions with proportionate civil penalties linked to unlawful gains or investor losses, while retaining strict punishment for market abuse. The Bill enhances investor protection through mandatory grievance redressal mechanisms and an Ombudsperson framework, and facilitates innovation via a regulatory sandbox.

(Link: Securities Market Code as introduced in Lok Sabha Dated 15/12/2025)

G. Ministry of Corporate Affairs (MCA)

Amendments to Companies Appointment and Qualification of Directors Rules - Director KYC Triennial Filing: The Companies (Appointment and Qualification of Directors) Rules, 2025 have been amended to provide procedural changes to director identification and KYC compliance. It mandates exclusive use of Form DIR-3 KYC-Web, discontinuing parallel references to e-forms and web services. A substituted Rule 12A now requires every individual holding a Director Identification Number (DIN) as on 31st March of a financial year to file KYC intimation once every third consecutive financial year by 30th June, rather than annually. Additionally, any change in a director's mobile number, email address, or residential address must be reported through DIR-3 KYC-Web within 30 days.

(Link: MCA Notification Dated 31/12/2025)

Amendments to Companies Removal of Names of Companies from Register of Companies Rules: A proviso has been added to rule 4(3), to provide that in case of any other Government Company, including its subsidiaries, the indemnity bond in Form STK-3A, in respect of one or more directors appointed or nominated by the Central Government or State Government, shall be given by an authorised representative not below the rank of Under Secretary or equivalent, in the administrative Ministry or Department of the Government of India or the State Government, as the case may be, on behalf of the Company.

(Link: MCA Notification Dated 31/12/2025)

Amendments to Companies Specification of Definition Details Rules: The significantly increased the financial thresholds for classifying a "Small Company," raising the paid-up capital limit to Rs 10 Crores (from Rs 4 Crore) and the turnover limit to Rs 100 Crores (from Rs 40 Crore), to reduce compliance burdens and encourage business growth by bringing more companies under beneficial, simplified governance rules.

(Link: MCA Notification Dated 01/12/2025)

MCA extends Annual Filing deadline without Additional Fees: The circular provides compliance relief to companies by extending the due date for filing financial statements and annual returns for FY 2024–25 without payment of additional fees. It provides that companies are now permitted to file key statutory e-forms—such as MGT-7, MGT-7A, AOC-4, AOC-4 CFS, AOC-4 (XBRL), and NBFC-specific AOC forms—up to 31 January 2026 with zero additional fees.

(Link: MCA General Circular 08/2025 Dated 30/12/2025)

G. Insolvency and Bankruptcy Board of India (IBBI)

Amendments to IBBI Insolvency Resolution Process for Corporate Persons (CIRP) Regulations: The amendment inserts a new Regulation 38 (3A), prescribing additional mandatory disclosures in every resolution plan. A resolution applicant must provide a detailed statement of beneficial ownership, disclosing all natural persons who ultimately own or control the applicant, along with the shareholding structure and jurisdiction of each intermediate entity, in a format to be specified by the Board through circulars. The resolution plan must also include an affidavit confirming whether the applicant is eligible or not eligible for the benefit of Section 32A of the Code.

(Link: IBBI Notification dared 22/12/2025)

Statement of Beneficial Ownership and Affidavit under CIRP Regulations: The circular prescribe mandatory formats for the Statement of Beneficial Ownership and an Affidavit on eligibility under section 32A of the IBC. It requires every resolution plan to disclose detailed beneficial ownership information of the Prospective Resolution Applicant (PRA) and to include a sworn affidavit clarifying whether the PRA is eligible for section 32A immunity. The Resolution Professional is expressly made responsible for ensuring that both documents form part of the resolution plan submitted to the Committee of Creditors and are filed before the Adjudicating Authority under section 30(6) of IBC.

(Link: IBBI Circular Dated 29/12/2025)

Form Modification Facility and Late Filing Fees introduced under CIRP Regulations: IBBI has introduced a modification utility on its electronic platform to allow Insolvency Professionals (IPs) to correct or update Corporate Insolvency Resolution Process (CIRP) forms already submitted. Where a form is initially filed and subsequently modified before the prescribed due date, no fee will be levied, as the computation of fees begins only after the due date. It has also announced the commencement of fees for delayed filing of CIRP forms under Regulation 40B of the CIRP Regulations.

(Link: IBBI Circular Dated 18/12/2025)

SC, Forfeiture of Rs 37.80 Crore upheld by because buyer missed timelines under IBC: Case of Shri Karshni Alloys Private Limited vs Ramakrishnan Sadasivan, SCJudgement Dated 10th December 2025. The apex court upheld the forfeiture of a purchaser deposit in a liquidation sale for failing to meet payment deadlines, emphasizing the NCLT authority to impose strict conditions to ensure timely resolution under the IBC.

(Link: SC Judgement Dated 10/12/2025)

SC, Development agreement which stood terminated prior to CIRP do not constitute asset of Corporate Debtor: Case of AA Estates Private Limited vs Kher Nagar Cooperative Housing Society Limited, SC Judgement Dated 28th November 2025. The apex court held that development right of a defaulting developer do not constitute 'asset' or 'property' of corporate debtor.

Further, since the said development agreement stood terminated prior to initiation of CIRP no subsisting or enforceable right survived in favour of corporate debtor.

(Link: SC Judgement Dated 28/11/2025)

NCLAT, Provisional Attachment order ceases by virtue of legislative scheme under section 32A of IBC: Case of Vantage Point Asset Management Pte Limited vs Gaurav Misra Resolution Professional of Alchemist Infra, NCLAT Delhi Judgement Dated 4th December 2025. The appellate tribunal held that that Provisional Attachment order has to be treated to cease by virtue of legislative scheme under Section 32A of the Insolvency and Bankruptcy Code and there is no necessity to obtain any order by the Successful Resolution Applicant (SRA) from the adjudicating authority under the PMLA.

(Link: NCLAT Delhi Judgement Dated 04/12/2025)

NCLAT, No limitation to look back when transaction held to be fraudulent under IBC: Case of Anubhav Anilkumar Aggarwal vs Rajendra Kumar Girdhar, NCLAT Delhi Judgement Dated 21st November 2025. The case involved a payment arrangement where 99% of the payment was required before the seller even owned the debt, which the appellate tribunal viewed as a pre-planned diversion of funds from the Corporate Debtor. It held that once a transaction has been held to a fraudulent transaction there is no limitation to look back if the other ingredients of Section 66 (1) of the Insolvency and Bankruptcy Code are satisfied.

(Link: NCLAT Delhi Judgement Dated 21/11/2025)

NCLAT, Release of Property cannot be denied without confirming ED attachment List: Case of Mohan Reddy Bhumi Reddy Gari vs STCI Finance Ltd, NCLAT Delhi Judgement Dated 18th November 2025. The appellate tribunal held that the NCLT committed a manifest illegality by failing to ascertain whether Flat No. 2402 was actually attached. Instead of deciding the issue, the NCLT shifted the responsibility onto the financial creditor and placed the burden on the appellant to secure release of the flat through undertakings. It clarified that if the property was indeed attached under the provisional attachment order, then the Supreme Court order would protect such attachment. If the property was not attached, the NCLT had full authority to order its release. It remanded the matter back for fresh adjudication.

(Link: NCLAT Delhi Judgement Dated 19/11/2025)

NCLAT, Prospective Resolution Applicant does not have vested right to challenge Approved Resolution Plan: Case of Astral Agro Ventures vs Vakati Balasubramaniyam Reddy, NCLAT Delhi Judgement Dated 18th November 2025. The appellate tribunal held that Prospective Resolution Applicant or unsuccessful Resolution Applicant does not have vested right to challenge a resolution process or an approved resolution plan.

(Link: NCLAT Delhi Judgement Dated 18/11/2025)

NCLAT, Gujarat State Tax Department is secured creditor hence direction to RP to release amount Justified: Case of Cosmos Coop Bank Ltd vs Kailash T Shah, NCLAT Delhi Judgement Dated 13th November 2025. The appellate tribunal held that direction to resolution professional to release the amount to Gujarat State Tax Department treating it as secured creditor under Section 48 of the Gujarat Value Added Tax Act, is justifiable as NCLT is obliged to apply decision of Supreme Court.

(Link: NCLAT Delhi Judgement Dated 13/11/2025)

NCLAT, Appeal by shareholder not maintained as shareholder is not person aggrieved under section 61 of IBC: Case of Peninsula Holdings and Investments Pvt Ltd vs JM Financial Credit Solutions Ltd, NCLAT Delhi Judgement Dated 29th October 2025. The appellate tribunal ruled that a shareholder is not a "person aggrieved" under Section 61 of the IBC and therefore lacks the standing (locus standi) to challenge the admission of a corporate debtor into the Corporate Insolvency Resolution Process (CIRP).

(Link: NCLAT Delhi Judgement Dated 29/10/2025)

NCLAT, Debt arising from advance to corporate debtor for supply of goods qualifies as Operational Debt: Case of Rakesh Bhailalbhai Patel vs Vasundhara Seamless Stainless Tubes Private Limited, NCLAT Delhi Judgement Dated 17th October 2025. The appellate tribunal held that debt arising from advance payment to corporate debtor for the supply of goods qualifies as operational debt under section 5(21) of the IBC. The operational debt and default established, hence section 9 application rightly admitted.

(Link: NCLAT Delhi Judgement Dated 17/10/2025)

NCLAT, Claim in CIRP rightly rejected since payments for flats to Corporate Debtor Not Established: Case of Sneha Kore vs Arun Kapoor, NCLAT Delhi Judgement Dated 17th September 2025. The appellate tribunal held that rejection of claim in CIRP of corporate debtor justified since Appellants failed to establish the crucial aspect of transfer of monies to the bank account of Corporate Debtor for purchase of flats.

(Link: NCLAT Delhi Judgement Dated 17/09/2025)

IBBI suspends Liquidator for arbitrary rejection of bids in Liquidation Auction: The DC noted that e-auction Bid Application Form granted the Liquidator broad discretionary powers to demand documents, accept or reject offers, cancel auctions, and determine the successful bidder. The DC held that these clauses conflicted with the statutory framework under Schedule I of the Liquidation Regulations, which requires transparent, reasoned decisions, including mandatory intimation of reasons when a highest bid is rejected. The second contravention related to the convening of the 6th SCC meeting, without even 24 hours' notice. Regulations require a minimum five-day notice for meetings, reducible to not less than 24 hours. DC suspended the registration of IP Amresh Shukla for six months.

(Link: IBBI DC Order dared 11/12/2025)

RTI Appeal rejected where Disclosure could impede ongoing Disciplinary Proceedings: The appellant had sought extensive information, including internal file notings, communications with Resolution Professional and the Committee of Creditors member bank, copies of the show cause notice, replies, hearing details, and status of disciplinary proceedings. The CPIO had informed that the complaint was admitted and disciplinary proceedings were initiated, but declined detailed disclosure. On appeal, the FAA held that most of the information sought was exempt under the RTI Act, as disclosure at this stage could impede ongoing disciplinary proceedings and any prosecution. However, FAA directed disclosure of file notings pertaining to the complaint.

(Link: IBBI ED&FAA RTI Order Dated 18/12/2025)

I. Reserve Bank of India (RBI)

Amendments to Banking Regulation (Co-operative Societies) Rules: The notification define an 'ineligible director' as one not meeting criteria under Section 10-A(2) of the Banking Regulation Act. A new Rule 5-A prescribes the procedure for determining, by drawing of lots, which ineligible directors or persons will cease to hold office or be removed from the Board, with the Reserve Bank authorized to oversee the process and allow the cooperative bank to nominate a representative.

Rule 11 is omitted, and reporting dates in FORM I and FORM IX are revised to the 15th and last day of the month.

(Link: FinMin Notification Dated 10/12/2025)

Amendments to Banking Regulation (Companies) Rules: The key changes include omission of references to 'subsidiary banks' in rules and forms, and removal of certain sub-clauses in rule 2, rule 2A, and rule 15B. Reporting timelines in FORM VIII and FORM X are revised from alternate Fridays to the 15th and last day of the month, aligning filings with a regular monthly schedule. Reporting formats have also been updated.

(Link: FinMin Notification Dated 10/12/2025)

Master Direction on RBI Rupee Interest Rate Derivatives Directions: The Directions govern the conduct of Interest Rate Derivatives (IRD) transactions in both over-the-counter (OTC) markets and on recognized stock exchanges, including Forward Rate Agreements, Interest Rate Swaps, Interest Rate Futures, caps, floors, collars, and swaptions. They define eligible participants, classify users into retail and non-retail, and set parameters for non- resident participation, including back-to-back arrangements and PVBP limits for hedging and other purposes. The Directions mandate reporting of all IRD transactions to the Trade Repository (CCIL), adherence to prudential norms, accounting standards, and risk management practices.

(Link: RBI Master Direction Dated 08/12/2025)

Compliance with Know Your Customer (KYC) norms: RBI has repealed the 2016 Master Direction on KYC and replaced it with the new "Reserve Bank of India (Commercial Banks– Know Your Customer) Directions, 2025".. All Payment System Providers and Participants must now align their KYC, AML, and CFT compliance processes with the updated 2025 framework. The changes include updated references to the new KYC Directions, revisions to digital KYC and V-CIP provisions, and harmonized requirements for OVDs, mandatory documents, and due diligence procedures.

(Link: RBI Notification 101/2025 Dated 28/11/2025)

Liberalised Remittance Scheme (LRS), Submission of 'LRS Daily Return' by Authorised Dealers: Presently, only AD Category-I banks submit daily LRS returns on the Centralised Information Management System (CIMS) and include LRS transactions of their attached AD Category-II banks and Full Fledged Money Changers (FFMCs). From January 2026 onwards, AD Category-II banks/entities and FFMCs will directly submit their own LRS daily returns, allowing them to monitor the cumulative PAN-wise LRS remittances of residents before approving new transactions.

(Link: RBI Notification 102/2025 Dated 03/12/2025)

Amendment to RBI Commercial Banks- Responsible Business Conduct Directions: It introduce major changes to the Basic Savings Bank Deposit (BSBD) framework. The amendments redefine "Digital Payment Transaction" and overhaul paragraphs 86 to 92, mandating banks to offer BSBD accounts as a standard service with essential facilities i.e. cash deposits, unlimited monthly deposits, ATM-cum-debit card without annual fees, a 25 leaf cheque book, internet/mobile banking, free passbook or e- statements, and four free withdrawals per month. Banks must not impose minimum balance requirements and must allow customers to convert existing accounts into BSBD accounts within seven days.

(Link: RBI Notification 103/2025 Dated 04/12/2025)

Amendment to RBI Small Finance Banks- Responsible Business Conduct Directions: Similar amendments refer above brief for notification 103/2025 dated 04/12/2025.

(Link: RBI Notification 104/2025 Dated 04/12/2025)

Amendment to RBI Payment Banks- Responsible Business Conduct Directions: Similar amendments refer above brief for notification 103/2025 dated 04/12/2025.

(Link: RBI Notification 105/2025 Dated 04/12/2025)

Amendment to RBI Local Area Banks- Responsible Business Conduct Directions: Similar amendments refer above brief for notification 103/2025 dated 04/12/2025.

(Link: RBI Notification 106/2025 Dated 04/12/2025)

Amendment to RBI Regional Rural Banks- Responsible Business Conduct Directions: Similar amendments refer above brief for notification 103/2025 dated 04/12/2025.

(Link: RBI Notification 107/2025 Dated 04/12/2025)

Amendment to RBI Urban Coop Banks- Responsible Business Conduct Directions: Similar amendments refer above brief for notification 103/2025 dated 04/12/2025.

(Link: RBI Notification 108/2025 Dated 04/12/2025)

Amendment to RBI Rural Coop Banks- Responsible Business Conduct Directions: Similar amendments refer above brief for notification 103/2025 dated 04/12/2025.

(Link: RBI Notification 109/2025 Dated 04/12/2025)

Amendment to RBI Commercial Banks- Credit Information Reporting Directions: It update existing directions to ensure systematic reporting by Commercial Banks to Credit Information Companies (CICs). Credit institutions (CIs) must submit credit information on four reference dates i.e. 9th, 16th, 23rd, and the last day of the month, with full-file submissions by the 5th of the following month, including active accounts and closed accounts since the last report. The directions also mandate reporting of Central KYC (CKYC) numbers and prompt correction of rejected data.

(Link: RBI Notification 110/2025 Dated 04/12/2025)

Amendment to RBI Small Finance Banks- Credit Information Reporting Directions: Similar amendments refer above brief for notification 110/2025 dated 04/12/2025.

(Link: RBI Notification 111/2025 Dated 04/12/2025)

Amendment to RBI Local Area Banks- Credit Information Reporting Directions: Similar amendments refer above brief for notification 110/2025 dated 04/12/2025.

(Link: RBI Notification 112/2025 Dated 04/12/2025)

Amendment to RBI Regional Rural Banks- Credit Information Reporting Directions: Similar amendments refer above brief for notification 110/2025 dated 04/12/2025.

(Link: RBI Notification 113/2025 Dated 04/12/2025)

Amendment to RBI Urban Coop Banks- Credit Information Reporting Directions: Similar amendments refer above brief for notification 110/2025 dated 04/12/2025.

(Link: RBI Notification 114/2025 Dated 04/12/2025)

Amendment to RBI Rural Coop Banks- Credit Information Reporting Directions: Similar amendments refer above brief for notification 110/2025 dated 04/12/2025.

(Link: RBI Notification 115/2025 Dated 04/12/2025)

Amendment to RBI All India Financial Institutions- Credit Information Reporting Directions: Similar amendments refer above brief for notification 110/2025 dated 04/12/2025.

(Link: RBI Notification 116/2025 Dated 04/12/2025)

Amendment to RBI Non-Banking Financial Companies- Credit Information Reporting Directions: Similar amendments refer above brief for notification 110/2025 dated 04/12/2025.

(Link: RBI Notification 117/2025 Dated 04/12/2025)

Amendment to RBI Asset Reconstruction Companies- Credit Information Reporting Directions: Similar amendments refer above brief for notification 110/2025 dated 04/12/2025.

(Link: RBI Notification 118/2025 Dated 04/12/2025)

Amendment to RBI Credit Information Companies Directions: Similar amendments refer above brief for notification 110/2025 dated 04/12/2025.

(Link: RBI Notification 119/2025 Dated 04/12/2025)

RBI Urban Co-operative Banks- Licensing, Scheduling and Regulatory Classification Repeal Guidelines: The previous Guidelines issued on 28th November 28, 2025 has been repealed and simultaneously replaced with a new set issued on the same day.

(Link: RBI Notification 120/2025 Dated 04/12/2025)

RBI Urban Coop Banks- Branch Authorisation Repeal Directions: The previous Directions issued on 28th November 28, 2025 has been repealed and simultaneously replaced with a new set issued on the same day.

(Link: RBI Notification 121/2025 Dated 04/12/2025)

RBI Rural Coop Banks- Branch Authorisation Repeal Directions: The previous Directions issued on 28th November 28, 2025 has been repealed and simultaneously replaced with a new set issued on the same day.

(Link: RBI Notification 122/2025 Dated 04/12/2025)

Amendment to RBI Rural Coop Banks- Miscellaneous Directions: The amended provisions mandate that all banks prominently display their full registered name, matching their Certificate of Registration and RBI licence, on all stationery, advertisements, websites, apps, and publicity material. Moreover, new norms have been prescribed for State Co-operative Banks seeking inclusion in the Second Schedule to the RBI Act, including higher CRAR requirements, absence of supervisory concerns, and submission of financial and governance documents through NABARD.

(Link: RBI Notification 123/2025 Dated 04/12/2025)

Amendment to RBI Commercial Banks- Credit Facilities Directions: The amendment introduce comprehensive changes to Gold Metal Loans (GML). It inserts definitions for GML, distinguishing between GMS-linked GML under the Gold Monetization Scheme, 2015, and import- linked GML sourced from imported gold. It also prescribe prudential guidelines for lending, risk management, monitoring, and repayment of GML to jewellery industry borrowers, including exporters and MMTC Limited. Banks must lay down lending policies, conduct due diligence, comply with capital adequacy requirements, and value GML in INR based on daily LBMA Gold rates.

(Link: RBI Notification 124/2025 Dated 04/12/2025)

Amendment to RBI Small Finance Banks- Credit Facilities Directions: The amendment introduce comprehensive changes to Gold Metal Loans (GML). It inserts definitions for GML, distinguishing between GMS-linked GML under the Gold Monetization Scheme, 2015, and import- linked GML sourced from imported gold. It also prescribe prudential guidelines for lending, risk management, monitoring, and repayment of GML to jewellery industry borrowers, including exporters and MMTC Limited. Banks must lay down lending policies, conduct due diligence, comply with capital adequacy requirements, and value GML in INR based on daily LBMA Gold rates.

(Link: RBI Notification 125/2025 Dated 04/12/2025)

Amendment to RBI Commercial Banks- Concentration Risk Management Directions: The key modifications include redefining "eligible capital base" to incorporate Tier I capital infusions and accrued profits, clarifying that branches in other jurisdictions are excluded from intra-group exposure limits except for proprietary derivatives, and enhancing board-level policies for monitoring ultra-large borrowers. It revise large exposures framework (LEF) norms, specifying exposure limits for Indian branches of foreign G-SIBs and non-G-SIBs, and mandate gross calculation of exposures cleared through central counterparties.

(Link: RBI Notification 126/2025 Dated 04/12/2025)

Amendment to RBI Small Finance Banks- Concentration Risk Management Directions: It emphasizes that small finance banks must have robust policies to manage concentration risk arising from exposures to single counterparties, interconnected groups, specific sectors, and ultra-large borrowers with substantial leverage. Banks may define "ultra-large borrowers" using their own criteria but must consider total borrowings from the banking system when assessing credit risk.

(Link: RBI Notification 127/2025 Dated 04/12/2025)

Amendment to RBI Commercial Banks- Income Recognition, Asset Classification and Provisioning Directions: The key change pertains to Paragraph 117 under Chapter IV relating to Provisioning Norms, which has been deleted. As a result, banks are now permitted to reverse provisions previously made or transfer them to the General Reserve. It aims to provide flexibility to banks in managing their provisioning practices while maintaining financial prudence.

(Link: RBI Notification 128/2025 Dated 04/12/2025)

Amendment to RBI Small Finance Banks- Income Recognition, Asset Classification and Provisioning Directions: The key change pertains to Paragraph 113 under Chapter IV relating to Provisioning Norms, which has been deleted. As a result, banks are now permitted to reverse provisions previously made or transfer them to the General Reserve. It aims to provide flexibility to banks in managing their provisioning practices while maintaining financial prudence.

(Link: RBI Notification 129/2025 Dated 04/12/2025)

Amendment to RBI Commercial Banks- Prudential Norms on Capital Adequacy Directions: The key amendment is the deletion of Paragraph 78 under Chapter IV relating to Risk Weighted Assets (RWAs), which provides the framework for calculating RWAs for commercial banks. It aims to streamline prudential norms for capital adequacy and aligns capital computation methodology with updated risk management practices.

(Link: RBI Notification 130/2025 Dated 04/12/2025)

Amendment to RBI Commercial Banks- Prudential Norms on Capital Adequacy Directions: The key amendment is the deletion of Paragraph 68 under Chapter IV relating to Risk Weighted Assets (RWAs), which provides the framework for calculating RWAs for commercial banks. It aims to streamline prudential norms for capital adequacy and aligns capital computation methodology with updated risk management practices.

(Link: RBI Notification 131/2025 Dated 04/12/2025)

Liquidity Adjustment Facility- Change in rates: MPC has decided to reduce the policy repo rate under the Liquidity Adjustment Facility (LAF) by 25 basis points from 5.50 per cent to 5.25 per cent with immediate effect. Consequently, the standing deposit facility (SDF) rate and marginal standing facility (MSF) rate stand adjusted to 5.00 per cent and 5.50 per cent respectively.

(Link: RBI Notification 132/2025 dated 05/12/2025)

Standing Liquidity Facility for Primary Dealers: The Standing Liquidity Facility provided to Primary Dealers (PDs) (collateralised liquidity support) would be available at the revised repo rate of 5.25 per cent.

(Link: RBI Notification 133/2025 dated 05/12/2025)

Penal Interest on shortfall in CRR and SLR requirements- Change in Bank Rate: The Bank Rate has been revised downwards by 25 basis points from 5.75 per cent to 5.50 per cent. Accordingly, all penal interest rates on shortfall in CRR and SLR requirements, which are specifically linked to the Bank Rate, also stands revised.The revised penal interest rates shall be Bank Rate plus 3.0 percentage points (8.50 per cent) or Bank Rate plus 5.0 percentage points (10.50 per cent) depending on duration of shortfall.

(Link: RBI Notification 134/2025 dated 05/12/2025)

Amendment to RBI Commercial Banks- Undertaking of Financial Services Directions: The amended provisions specify that core banking functions and acceptance of time deposits must be undertaken departmentally, while mutual fund, insurance, pension, and portfolio management services must be conducted via group entities. The directions impose prudential investment limits i.e. a single bank may invest up to 10% in any entity, and aggregate investments, including group and overseas entities, may not exceed 20%, with prior approval required for higher exposures. Specific restrictions on Asset Reconstruction Companies, Alternative Investment Funds, and Real Estate/Infrastructure Investment Trusts have been provided.

(Link: RBI Notification 135/2025 Dated 05/12/2025)

Amendment to RBI Small Finance Banks- Undertaking of Financial Services Directions: The amendment specify that banks can act as agents for regulated third-party products but cannot handle referral processes directly. It clarifies that certain financial services, such as mutual funds, insurance, pension fund management, investment advisory, portfolio management, and broking, must be undertaken through a group entity under a Non-Operating Financial Holding Company (NOFHC), not departmentally. It also revises equity investment limits for banks, including individual and aggregate investment caps, investment conditions, and reporting requirements.

(Link: RBI Notification 136/2025 Dated 05/12/2025)

Amendment to RBI Payment Banks- Undertaking of Financial Services Directions: The amendments allow banks to act as agents of third-party product or service providers (TPPSPs) for regulated financial products, including insurance, mutual funds, and pensions, without assuming risk. It outlines responsibilities such as marketing, sales, customer support, and after-sale services. Moreover, Referral Services permit Payments Banks to refer customers to TPPSPs without involvement in product processes or branding, ensuring operational separation and compliance.

(Link: RBI Notification 137/2025 Dated 05/12/2025)

Amendment to Non-Banking Finance Companies- Undertaking of Financial Services Directions: The amendment insert new paragraph 60A, which mandates that NBFCs forming part of a Scheduled Commercial Bank group must also comply with the Commercial Banks– Undertaking of Financial Services Directions, 2025 whenever both the NBFC and the parent bank engage in the same business activity. This ensures uniform regulatory treatment, prevents regulatory arbitrage, and strengthens governance and oversight across bank-led financial conglomerates.

(Link: RBI Notification 138/2025 Dated 05/12/2025)

Amendment to Non-Operative Financial Holding Company (NOFHC) Directions: The amendments replace paragraphs 44– 47, reiterating that all activities permitted to banks under Banking Regulation Act, must be undertaken directly by the bank. Specialized activities, such as mutual funds, insurance, pension fund management, investment advisory, portfolio management, and broking, must be conducted only through subsidiaries, joint ventures, or associates. NOFHCs are not required to seek prior RBI approval for these specified activities, but must notify the RBI within 15 days of board resolution.

(Link: RBI Notification 139/2025 Dated 05/12/2025)

Export and Import of Indian Currency to or from Nepal and Bhutan: The new guidelines allow any person, except citizens of Pakistan or Bangladesh, to carry Indian currency notes in specific limits. Currency denominations up to Rs 2,100 can be freely moved across the border, while higher denominations (above Rs 2,100) can be exported or imported up to a total limit of Rs 2,25,000. The amendment under FEMA Export and Import of Currency Regulations was notified on 2nd December 2025.

(Link: RBI Notification 140/2025 Dated 08/12/2025)

Amendment to RBI Commercial Banks- Credit Risk Management Directions: The amendments introduce provisions regarding maintenance of Cash Credit (CC), Current, and Overdraft (OD) accounts to strengthen credit monitoring and discipline. CC accounts remain operationally linked to working capital needs, while current and OD accounts may be maintained freely by customers with banking system exposure below Rs 10 crore. For exposures of Rs 10 crore or more, only banks with minimum 10% exposure or the largest lenders may maintain such accounts, others are restricted to collection accounts. Collection accounts must transfer funds to designated accounts within two working days.

(Link: RBI Notification 141/2025 Dated 11/12/2025)

Amendment to RBI Small Finance Banks- Credit Risk Management Directions: Similar amendments refer above brief for notification 141/2025 dated 11/12/2025.

(Link: RBI Circular 142/2025 Dated 11/12/2025)

Amendment to RBI Payment Banks- Miscellaneous Directions: The amendment defines Current Account to include demand deposits not classified as savings or term deposits. Banks may maintain unrestricted current accounts for borrowers with aggregate banking system exposure below Rs 10 crore, while customers with exposure of Rs 10 crore or more must operate collection accounts, with funds remitted within two working days to a designated account.

(Link: RBI Notification 143/2025 Dated 11/12/2025)

Amendment to RBI Regional Rural Banks- Credit Risk Management Directions: Similar amendments refer above brief for notification 141/2025 dated 11/12/2025.

(Link: RBI Notification 144/2025 Dated 11/12/2025)

Amendment to RBI Local Area Banks- Credit Risk Management Directions: Similar amendments refer above brief for notification 141/2025 dated 11/12/2025.

(Link: RBI Notification 145/2025 Dated 11/12/2025)

Amendment to RBI Urban Cooperative Banks- Credit Risk Management Directions: Similar amendments refer above brief for notification 141/2025 dated 11/12/2025.

(Link: RBI Notification 146/2025 Dated 11/12/2025)

Amendment to RBI Rural Cooperative Banks- Credit Risk Management Directions: Similar amendments refer above brief for notification 141/2025 dated 11/12/2025.

(Link: RBI Notification 147/2025 Dated 11/12/2025)

Amendment to RBI Commercial Banks- CRR and SLR Directions: The directions redefine 'Fortnight' for CRR and SLR maintenance from 'Saturday to second following Friday' to 'first to fifteenth day or sixteenth to last day of each calendar month'. Reporting requirements are revised, mandating a single Form A return fortnightly and For VIII return monthly via the CIMS portal in electronic format with digital signatures.

(Link: RBI Notification 148/2025 Dated 11/12/2025)

Amendment to RBI Small Finance Banks- CRR and SLR Directions: Similar amendments refer above brief for notification 148/2025 dated 11/12/2025.

(Link: RBI Notification 149/2025 Dated 11/12/2025)

Amendment to RBI Payments Banks- CRR and SLR Directions: Similar amendments refer above brief for notification 148/2025 dated 11/12/2025.

(Link: RBI Notification 150/2025 Dated 11/12/2025)

Amendment to RBI Regional Rural Banks- CRR and SLR Directions: Similar amendments refer above brief for notification 148/2025 dated 11/12/2025.

(Link: RBI Notification 151/2025 Dated 11/12/2025)

Amendment to RBI Local Area Banks- CRR and SLR Directions: Similar amendments refer above brief for notification 148/2025 dated 11/12/2025.

(Link: RBI Notification 152/2025 Dated 11/12/2025)

Amendment to RBI Urban Cooperative Banks- CRR and SLR Directions: Similar amendments refer above brief for notification 148/2025 dated 11/12/2025.

(Link: RBI Notification 153/2025 Dated 11/12/2025)

Amendment to RBI Rural Cooperative Banks- CRR and SLR Directions: Similar amendments refer above brief for notification 148/2025 dated 11/12/2025.

(Link: RBI Notification 154/2025 Dated 11/12/2025)

Assignment of Lead Bank Responsibility for new district Vav-Tharad in Gujarat: The Lead Bank Responsibility for new district i.e Vav-Tharad in the state of Gujarat has been assigned to Bank of Baroda.

(Link: RBI Notification 155/2025 Dated 18/12/2025)

Continuous Cheque Clearing and Settlement Phase 2 is Deferred: The circular related to changes to the rollout of Continuous Clearing and Settlement on Realisation (CCSR) in the Cheque Truncation System (CTS). While Phase 1 was implemented on 4th October 2025, Phase 2 has been postponed until further notice to provide banks additional time to streamline operational processes. It has also revised the CTS timelines by rescheduling the presentation session to 9:00 AM–3:00 PM and the confirmation session to 9:00 AM–7:00 PM.

(Link: RBI Notification 156/2025 Dated 24/12/2025)

Amendment to RBI All India Financial Institutions- Know Your Customer Directions: The amendment clarify the accountability for customer verification within the Central KYC Records Registry (CKYCR) framework. It has been specified that the regulated entity which last uploads or updates a customer's KYC record in CKYCR shall be responsible for verifying the customer's identity and/or address. Consequently, All India Financial Institutions (AIFIs) that download and rely on current and PML-compliant CKYCR records are not required to re-verify identity or address.

(Link: RBI Notification 157/2025 Dated 29/12/2025)

Amendment to RBI Asset Reconstruction Companies- Know Your Customer Directions: Similar amendments refer above brief details for notification 157/2025 dated 29/12/2025.

(Link: RBI Notification 158/2025 Dated 29/12/2025)

Amendment to RBI Local Area Banks- Know Your Customer Directions: Similar amendments refer above brief details for notification 157/2025 dated 29/12/2025.

(Link: RBI Notification 159/2025 Dated 29/12/2025)

Amendment to RBI Non-Banking Financial Companies- Know Your Customer Directions: Similar amendments refer above brief details for notification 157/2025 dated 29/12/2025.

(Link: RBI Notification 160/2025 Dated 29/12/2025)

Amendment to RBI Payments Banks- Know Your Customer Directions: Similar amendments refer above brief details for notification 157/2025 dated 29/12/2025.

(Link: RBI Notification 161/2025 Dated 29/12/2025)

Amendment to RBI Regional Rural Banks- Know Your Customer Directions: Similar amendments refer above brief details for notification 157/2025 dated 29/12/2025.

(Link: RBI Notification 162/2025 Dated 29/12/2025)

Amendment to RBI Rural Cooperative Banks- Know Your Customer Directions: Similar amendments refer above brief details for notification 157/2025 dated 29/12/2025.

(Link: RBI Notification 163/2025 Dated 29/12/2025)

Amendment to RBI Small Finance Banks- Know Your Customer Directions: Similar amendments refer above brief details for notification 157/2025 dated 29/12/2025.

(Link: RBI Notification 164/2025 Dated 29/12/2025)

Amendment to RBI Urban Cooperative Banks- Know Your Customer Directions: Similar amendments refer above brief details for notification 157/2025 dated 29/12/2025.

(Link: RBI Notification 165/2025 Dated 29/12/2025)

Amendment to RBI Commercial Banks- Know Your Customer Directions: Similar amendments refer above brief details for notification 157/2025 dated 29/12/2025.

(Link: RBI Notification 166/2025 Dated 29/12/2025)

Withdrawal of Rs 2000 Denomination Banknotes Status: The Reserve Bank of India (RBI) had announced the withdrawal of Rs 2000 denomination banknotes from circulation vide Press Release dated 19th May 2023. These notes can be exchanged/ deposited/ send through India Post from any post office in the country, to any of the 19 RBI Issue Offices for credit to their bank accounts in India. The ₹2000 banknotes continue to be legal tender. The total value of Rs 2000 banknotes in circulation, which amounted to Rs 3.56 lakh crore, has declined to Rs 5743 crore as at the close of business on 29th November 2025. Thus, 98.39% of the banknotes has since been returned.

(Link: RBI Press Release Dated 01/12/2025)

J. Miscellaneous

ESIC Registration mandated after Social Security Code Rollout: The Code on Social Security has been implemented with effect from 21st November 2025, consolidating social security laws to provide medical and financial protection to employees across all establishments. The registration with the Employees State Insurance Corporation (ESIC) has become mandatory for all establishments meeting the prescribed criteria, including educational and medical institutions. The notification reiterates that the new definition of "wages" under the Code includes only basic pay, dearness allowance, and retaining allowance, if any.

(Link: ESIC Circular Dated 10/12/2025 and 11/12/2025)

SC, No Arbitration without privity: Case of Hindustan Petroleum Corporation Limited vs BCL Secure Premises Pvt Ltd, SC Judgement Dated 9th December 2025. The apex court held that the referral court should be prima facie satisfied that there exists an arbitration agreement and as to whether the non-signatory is a veritable party. The apex court opined that the referral court under Section 11 is not deprived of its jurisdiction from examining whether the non-signatory is in the real sense a party to the arbitration agreement. SC held that BCL did not establish its case to show even prima facie, the existence of an arbitration agreement between HPCL and BCL. Thus, it set aside the HC judgment.

(Link: SC Judgement Dated 09/12/2025)

SC, Cash Loan above Rs 20,000 not a defence to Cheque Bounce: Case of Shine Varghese Koipurathu vs State of Kerala,SC Judgement Dated 8th December 2025. The apex court held that a cash loan over Rs 20,000, even if violating Income Tax Act (Section 269SS), remains a legally enforceable debt for Section 138 of Negotiable Instrument Act (cheque bounce) cases. The court held that violations of the Income Tax Act for large cash transactions result in separate penalties, not invalidation of the underlying financial obligation for cheque bounce proceedings.

(Link: SC Judgement Dated 08/12/2025)

SC, Nominee not absolute owner, divides GPF 50% each between Wife and Mother: Case of Smt Balla Malathi vs B Suguna, SC Judgement Dated 5th December 2025. The apex court held that the mother's pre-marriage GPF nomination became invalid after the employee got married. It further held that the funds must be equally shared between the wife and mother.

(Link: SC Judgement Dated 05/12/2025)

SC, FIR set aside because loan default lacked Entrustment: Case of Sunil Sharma vs Hero Fincorp Limited, SCJudgement Dated 12th August 2025. The apex court ruled that mere failure to repay loan in a commercial transaction is a civil liability, not a criminal offense, quashing criminal proceedings (FIR) for criminal breach of trust (Section 406 IPC) as an abuse of process, highlighting that dishonest intention (mens rea) is essential for criminal liability, which was not proven.

(Link: SC Judgement Dated 12/08/2025)

HC, Mark 'SoEasy' being suggestive in nature is liable to be protected under Trade Marks: Case of Ashim Kumar Ghosh vs Registrar of Trade Marks, HC Delhi Judgement Dated 24th November 2025. The court held that the mark 'SoEasy' for Hindi language learning is suggestive in nature and it is settled law that suggestive Trade Marks are liable to be protected under the Trade Marks Act, 1999. Accordingly, appeal is allowed

(Link: HC Delhi Judgement Dated 27/11/2025)

Disclaimer

The contents of this article are for informational purposes only. The user may refer to the relevant notification/ circular/ decisions issued by the respective authorities for specific interpretation and compliances related to a particular subject matter)

CMA Yash Paul Bhola

MBA, CMA
Former Director (Finance),
National Fertilizers Limited.

Social Entrepreneurship

The Perspective

India is a complex market and just money is not enough to navigate it. India has a strong impact investor base and in case you want to operate in this country, you would need to have money that is capable to help you navigate contextual challenges. There are trusted forums, investor councils and a strong network of stakeholders involved in the ecosystem

There is an important difference, however, between corporations that donate to charity or give back to their communities, and businesses that have made social responsibility their mission and guiding light. Businesses that fall into this category practice what is known as social entrepreneurship, and they are becoming more profitable and popular than ever before. While traditional businesses might measure success in terms of market share or year-over-year revenue growth, social entrepreneurs are more likely to focus on metrics like jobs created, trees planted, or donations made to a charitable arm that solves the problem they've invested in. A social entrepreneur, then, is someone who starts and builds a business that prioritizes the greater good. That is not to say that social entrepreneurs don't care about profits, because of course they do, but they care just as much about pursuing solutions that solve social and community problems and effect positive change.

What is social entrepreneurship?

Social entrepreneurship — born out of the cooperative movement that began in nineteenth-century Europe — gained traction in the 1980s and 1990s with the emergence of the social innovation and social enterprise schools of thought and practice. However, the principles of social entrepreneurship have guided the actions of philanthropists, including those who are now called venture philanthropists, for centuries. The rise of social entrepreneurship should be examined within the context of the broader paradigm shift in business and employment. An important aspect of this change relates to the growing importance of both internal and external social capital for enterprises in general. Social capital can be viewed as "the links, shared values and understandings in society that enable individuals and groups to trust each other and so work together.

Social entrepreneurs blend business with purpose. Their mission? To tackle pressing issues like poverty, education gaps, health care disparities, and environmental challenges — all while running a successful business. These innovators see problems as opportunities, using creative solutions to drive real, lasting impact. A social entrepreneur is a business leader who sees opportunity in solving some of society's biggest challenges. Whether it's protecting the environment, uplifting underserved communities, or launching philanthropic endeavours, these change makers are proving that success isn't just measured in revenue, but in real-world impact. Social entrepreneurship is a new, innovative business venture that influences change. Social entrepreneurs have a specific cause they care about, and they develop a business model around making a positive impact. The main goal is to create lasting social change through business. Social entrepreneurship can operate as a non-profit, for-profit, or hybrid business, depending on your preferred business model and the funding availability.

Some key areas of interest for social entrepreneurs include:

- Economic development
- Education
- Gender equality
- Healthcare
- Agriculture
- Environmental sustainability
- Renewable energy
- Community development

Entrepreneurship vs. social entrepreneurship

Social enterprises, blend profit with purpose. They run businesses that solve social or environmental problems while generating revenue. Unlike non-profits, they are not necessarily dependent on donations, and they can generate a profit from the goods or services they sell.

Like entrepreneurs, social entrepreneurs aim to create a sustainable business that lasts. However, while an entrepreneur aims to maximise profits, a social entrepreneur's primary concern is impact. Most other differences between the two types of entrepreneurship derive from that focal point.

	Entrepreneur	Social entrepreneur
Objective	Build a sustainable business	Build a sustainable and socially impactful business
Motive	Financially driven	Mission-driven
Focus	Individual consumers	Social groups
Link to social issues	Indirect	Direct
Competition/collaboration	Competitive with related businesses	Collaborative with related businesses
Success	Based on sustainable profits	Based on sustainable social impact

What are the different types of social entrepreneurship

Just as there are near-infinite expressions of entrepreneurship, there are countless forms social entrepreneurship can take. You could start a non-profit that provides funding for underserved entrepreneurs. Or you could launch a for-profit business that manufactures eco-friendly products. No matter what type of social entrepreneurship you choose, you'll need to be passionate about your cause and have a strong commitment to making a difference. With hard work and dedication, you can make a real impact on the world.

The different models you can adopt as a social entrepreneur include:

- **Non-profit:** A tax-exempt, non-business entity that invests excess funds back into the mission.
- **Co-operative:** A business organized by and for its members. Credit unions and community grocery stores are some examples of co-ops.
- **Social purpose business:** These businesses start on the foundation of addressing a social mission.
- **Social firm:** Social firms employ those in the community who need jobs, such as at-risk youth.
- **Socially responsible business:** These companies support social missions as a part of their day-to-day business operations.
- **For-profit:** Perhaps the vaguest category, these businesses are profit-first but donate funds, raise awareness, or otherwise support causes.

Starting a social enterprise

Starting a social enterprise means building a business that prioritizes impact as much as profit. Here are the key steps to get started:

- **Identify a social problem:** Determine the issue your business will address—whether it's poverty, education, sustainability, or another cause—ensuring it's something you're passionate about solving.

- **Develop a business model with impact:** Unlike traditional businesses, social enterprises integrate profit with purpose. Decide whether you'll operate as a non-profit, for-profit, or hybrid model while ensuring your revenue stream supports long-term change.
- **Create a sustainable business plan:** Outline your mission, financial strategy, and operational structure. Ensure your plan includes how your business will maintain its social impact while remaining financially viable.
- **Secure funding and resources:** Social enterprises often rely on impact investors, grants, crowd funding, or earned revenue. Research funding opportunities that align with your mission.
- **Measure and communicate impact:** Transparency is key. Track and share your social and environmental impact to build credibility and attract loyal customers, investors, and partners.

Do social entrepreneurs make money?

Social entrepreneurs do indeed make money. While most social entrepreneurs start out with modest goals to prioritize their mission first, many are eventually able to achieve financial success similar to traditional entrepreneurs. Even founders of non-profit organizations can eventually pay themselves a salary with certain limitations. The pursuit of profit and purpose are not mutually exclusive in business,

Create positive change through social entrepreneurship

Our connected world has brought about a new era of awareness, where we can find problems to solve and lives to improve across the street or across the world if we choose.

People from all over are deciding to make change in whatever way they can, whether it's by being more conscious of what they buy as consumers or building an engine for social and environmental good by becoming entrepreneurs.

The overall goal of social entrepreneurship is to facilitate sustainable development. Whether the company's focus is on improving access to employment of disenfranchised individuals or reducing their carbon footprint, the focus on improved social outcomes targets sustainable development for communities.

A lot of companies are already doing this and are actually working toward certain sustainable development goals without even realizing it. There are companies that are making decisions to reduce their environmental impact and others working along the lines of poverty reduction because they feel it's the right thing to do.

Social entrepreneurship examples in India

Social entrepreneurship in India tackles issues from poverty to education with innovative models :

Education & Livelihoods

- **Akanksha Foundation/Teach for India (Shaheen Mistri):** Providing quality education and skills training to children from low-income backgrounds.
- **Pratham Education Foundation (Madhav Chavan):** Delivering quality education to underprivileged children across India.
- **LabourNet Services (Gayathri Vasudevan):** Training and supporting informal sector workers for better employment.
- **Resham Sutra:** Empowering rural silk artisans with solar-powered machines to increase income and improve working conditions.

Health & Wellness

- **Arvind Eye Care System:** Offering high-quality, affordable eye care, restoring vision for millions.
- **Jaipur Foot:** Providing affordable prosthetic limbs to persons with disabilities.

Sustainable Energy & Environment

- **SELCO India (Harish Hande):** Delivering sustainable energy solutions (like solar) to the poor for improved quality of life.
- **Frontier Markets (Ajaita Shah):** Using women entrepreneurs to distribute clean energy products in rural households.
- **Pollinate Group:** Empowering women entrepreneurs to distribute clean energy in underserved areas.

Women's Empowerment & Micro-enterprise

- **Shri Mahila Griha Udyog Lijjat Papad:** A women's cooperative that revolutionized the papad industry, creating economic independence.
- **I was a Sari (Stefano Funari):** Transforming recycled saris into high-end fashion, empowering underprivileged women.
- **Mann Deshi Foundation:** Providing financial services and entrepreneurship support to rural women.

Finance & Community

- **SKS Microfinance:** Providing microfinance to underserved communities (early success, later faced challenges).
- **Rang De:** Peer-to-peer lending platform for low-cost loans to underserved communities.
- **AMUL Dairy Cooperative:** A classic example of a cooperative lifting dairy farmers out of poverty.

Conclusions

Social entrepreneurship must be seen as one of a wide range of development strategies, and it comes with a number of caveats. Indeed, successful entrepreneurship is rare, with the vast majority of entrepreneurs failing to provide the major innovations or creative destruction that can drive economic growth. It follows that promoting social entrepreneurship, and especially youth social entrepreneurship, is not a simple endeavour. With the appropriate support, social entrepreneurship may be a viable option for many youth, but it is not a panacea for the development and employment challenges young people face. It is especially important that the State and other relevant actors be prepared to provide long-term support, as potential entrepreneurs — particularly young people — need time to learn and build the necessary skills and experience to sustain successful social enterprises.

CMA (Dr.) S K Gupta

Chief Executive Officer
ICMAI Social Auditors Organization

Implementing AI and Automation: Practical, Low-Cost Ways MSMEs Can Use AI for Customer Service, Data Analysis, and Workflow Automation

Why AI and Automation Matter Now

Picture a small manufacturing supplier racing to fulfill a government tender. Employees sift through piles of paperwork to track orders, manually respond to repeated customer inquiries about delivery status, and crunch numbers in spreadsheets to estimate costs. Work gets delayed, errors creep in, and the team feels stretched. Now imagine this same business a year later: routine queries are handled instantly by a chatbot, invoices auto-fill into the system, and software predicts which raw materials to restock. This isn't science fiction – it's the reality that artificial intelligence (AI) and automation can create for micro, small, and medium enterprises (MSMEs) today.

What is AI, and what is automation?

In simple terms, automation means using technology to perform tasks with minimal human intervention – like an email program automatically sorting messages into folders. AI refers to computers mimicking human intelligence – learning from data and making decisions. For example, a basic automation might follow a fixed rule ("forward all invoices to accounts@business.com"), whereas an AI-based system can learn to flag unusual invoices by comparing thousands of past records. These technologies are increasingly common in everyday tools – think of voice assistants that understand commands, or smartphone apps that can translate signs just by viewing them.

Why does this matter for MSMEs right now?

Because AI and automation are no longer expensive, experimental concepts only for big companies. They are becoming accessible and affordable for small businesses, and the payoff can be significant. Studies have found that AI can dramatically cut costs and improve efficiency. For instance, a 2025 World Economic Forum report noted AI could reduce product costs by up to 32%, cut operating costs by 24%, and even reduce defects by 99% with advanced quality control. Even modest steps can yield results – initial pilots with AI in Indian MSMEs boosted productivity by 20% and lowered costs by 30%.

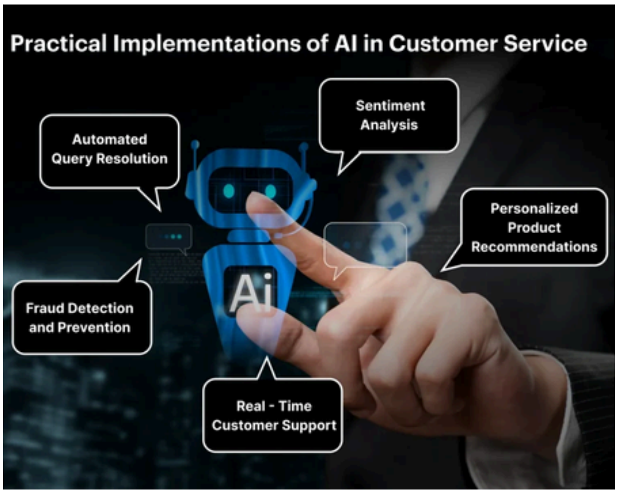
And it's not just one or two cases: across the world, small businesses are adopting AI to stay competitive. In 2024 about 40% of small businesses in the US were already using some AI tools, and by 2025 around 77% of small firms worldwide had integrated AI into at least one function. India is no exception – in fact, one survey found India leading in small business AI adoption, with about 59% of Indian SMBs already implementing AI-driven solutions. The takeaway is clear: AI and automation aren't just buzzwords; they're practical tools that can help even a 5-person company save time, cut errors, and grow.

Basics of AI and Automation – Without Jargon

Let's start with the basics. Traditional rule-based automation follows explicit instructions: you set the rules, and the computer faithfully repeats them. A classic example is an Excel macro that, when run, always formats a report the same way, or an email filter that moves any message with "[URGENT]" in the subject to a priority folder. This kind of automation is powerful for structured, repetitive tasks, and many MSME managers are already using it (perhaps without realizing) – for example, using formula-driven Excel sheets, or setting up auto-responders on email and WhatsApp for common queries.

AI-based automation, on the other hand, is like a smart apprentice that learns patterns and makes some decisions on its own. Rather than you coding every rule ("if customer asks X, respond with Y"), an AI system can observe lots of data and figure out the best response or action. For instance, an AI customer service tool can analyze hundreds of past support tickets and learn how to answer a question about late deliveries – even if the question is phrased in a way it hasn't seen before. Or consider your phone's keyboard that suggests the next word as you type – it's learned from millions of sentences (and your own typing habits) to predict what you might say. The key difference is flexibility: AI systems adapt based on experience, whereas traditional automation does exactly what it's told, and nothing more.

The good news for small businesses is that you don't need a big IT team or deep technical expertise to start automating. Many tools today come with AI "under the hood." If you've used Gmail's auto-complete suggestions or Google Translate, you've already touched AI. There are simple services that can read text from images (handy for digitizing bills), or smartphone apps that can understand spoken requests in Hindi or Tamil and fetch information.



Low-Cost AI Use Cases for Customer Service

One area where AI can immediately help MSMEs is customer service, and it doesn't require a massive investment. Imagine you run a small e-commerce operation supplying components to a large PSU or corporate. You likely get many repetitive questions: "Has my order shipped?" "When will it arrive?" "How do I get an invoice copy?" Responding to each query individually takes time – and missing a question can mean an unhappy client. Here are some practical, low-cost AI solutions that can lighten the load:

- **Chatbots for FAQs:** You can deploy a chatbot on your website or even on WhatsApp to answer frequently asked questions around the clock. Modern AI chatbots can handle questions about orders, delivery status, pricing, or product availability by pulling information from your database. For example, a textile MSME owner set up a WhatsApp chatbot that customers of all his retail clients can ping for order tracking; it instantly replies with the latest status, even at midnight when no staff are available. This kind of bot can be built without coding – many services offer plug-and-play chatbot templates for small businesses. It's often as simple as feeding the bot a Q&A list or connecting it to your Excel inventory sheet.
- **Automatic Ticketing and Routing:** For more complex queries or complaints, AI can triage and route requests to the right person. Let's say a customer sends an email that sounds angry and mentions a delayed shipment. AI text analysis can flag this as "high priority" and automatically create a support ticket. A rule-based system could assign it to the logistics manager if it contains words like "delivery" or to the finance team if "payment" is mentioned. Some affordable helpdesk tools for MSMEs use AI to categorize tickets (billing vs. technical issue vs. general inquiry) and even draft initial responses. The benefit is that nothing falls through the cracks, and the customer gets at least an acknowledgment immediately.
- **24/7 Multilingual Support:** If you serve diverse customers (think of an MSME supplying goods to different state governments or clients across India), you'll get inquiries in English, Hindi, Tamil, Bengali – depending on who's comfortable in which language. AI translation and natural language processing can bridge the gap. You could have a single chatbot that customers type to in any major Indian language; the AI interprets the question, finds the answer (e.g., in English internally), and responds in the customer's language. This was nearly impossible for small businesses a few years ago, but now services like Google's Dialogflow or Microsoft's Bot Framework support multilingual setups out of the box. It means your customer service is no longer confined to business hours or specific languages.

These customer service improvements directly impact client satisfaction. When MSMEs respond faster and more consistently, it builds trust – especially when serving large clients like PSUs or MNCs who often require timely communication. The data backs this up: 95% of small businesses that adopted AI-driven customer service report improved response quality, and 92% achieved faster response times for customers[6]. Consider a real example: a small auto-parts supplier in Pune integrated a chatbot into their order system for a major automotive MNC client. The chatbot could instantly answer that client's plant engineers about whether a part had been dispatched or if a shipment was delayed. Not only did this reduce late-night phone calls, but the MSME owner says it also won them more orders – the MNC's procurement team saw them as a proactive, tech-enabled vendor. In summary, AI can help even a tiny customer support team appear "big" – always available, responsive in any language, and quick to resolve issues – all at a relatively low cost.

AI for Data Analysis and Decision Making

Every MSME sits on a goldmine of data – whether it's sales figures in a ledger, production output numbers in an Excel file, or customer feedback emails in an inbox.

AI can turn this raw data into useful insights, often with minimal manual effort, helping owners and managers make better decisions. Here's how businesses can start, from basic steps to more advanced applications:

- **Automated Reports and Dashboards:** Many small businesses still spend days at month-end preparing reports – aggregating sales, tallying expenses, calculating how much each project earned. AI and automation can handle a lot of this grunt work. For instance, if you use an accounting software or even Excel, you can set up automated reporting that generates an up-to-date dashboard every morning. Cloud-based tools like Zoho Analytics or Microsoft Power BI (which have affordable plans) can pull data from your Excel sheets or Tally system and display key metrics – sales trends, pending receivables, inventory levels – in easy charts. Instead of poring over rows of numbers, you get visuals and alerts (e.g., "revenue 10% down this week"). This not only saves time but also ensures you catch issues early. A finance manager at a small manufacturing firm described how they scheduled an auto-generated weekly cash flow report emailed to the team – it freed her from manually updating the figures, and she could focus on interpreting why cash flow was low in a given week.

- **Predictive Analytics (Forecasting):** Going a step further, AI can analyze past patterns to predict future outcomes, which is incredibly useful for decision-making. Even if you only have two years of sales data, an AI tool might detect seasonality or growth trends that manual analysis could miss. For example, say you run a food processing unit. An AI service could examine your monthly sales and point out that demand spikes every October (maybe due to festival season), predicting how much inventory you'll need next October. It might even combine past data with other factors (like rainfall, if you're an agri-producer) to forecast yields or sales. Many MSME-focused ERP and accounting systems now have built-in forecasting modules. Predictive sales and demand forecasting can prevent stockouts or overproduction. If an AI model tells a textile wholesaler "Expect a 15% rise in orders for wool products in winter based on trends," they can stock up intelligently. In fact, a recent survey showed 45% of small businesses are very likely to adopt AI tools that predict revenue or demand trends – because anticipating the future, even imperfectly, is better than flying blind.

- **Financial Planning and Analysis:** AI isn't just for sales; it's a boon for finance and accounting professionals like Chartered Accountants (CAs) or Cost Accountants (CMAs) in MSMEs. Think of cash-flow prediction – a small business often lives or dies by its cash flow. AI tools can analyze your payment receivables, upcoming bills, and past client payment behavior to warn, "next month you may face a cash crunch because a big client typically pays late." This gives you a chance to arrange a credit line in advance. In one case, a distributor used an AI add-on with their accounting software which scanned all past invoices and bank statements to flag that certain customers usually delay payments beyond 60 days. The system now automatically highlights these "slow payers" and even suggests an increased provision for bad debts. No surprise, 53% of SMB finance teams see AI-based cash flow forecasting as a critical help for their work. Similarly, AI can assist in credit risk signals – for instance, scanning news or social media for signals about a major client (if news breaks that the client is in trouble, the AI can alert you to be cautious on extending credit).

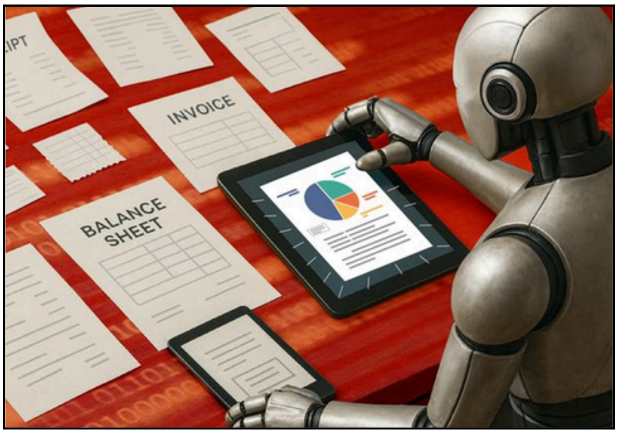
- **Anomaly Detection (Finding the "Odd One Out"):** This is like having a diligent auditor working 24/7. AI can watch your transactions and flag anything unusual. For example, if your average electricity bill is ₹50,000 and one month it shoots to ₹1,50,000, an automated system can send an alert – maybe a machine was left running, or there's a billing error. Or in procurement, if prices of a certain raw material suddenly double on an invoice, an AI might point it out for review ("Is this a typo or did prices really jump?"). Small accounting errors or even fraud can be caught this way. One MSME owner who runs a chain of retail stores implemented a simple AI tool to monitor daily sales and expenses from each outlet. One month, it flagged an "anomaly" – an abnormally high number of refunds at one store. On investigation, it turned out to be a billing software issue. Catching it early saved them from weeks of revenue leakage. AI's ability to sift through tons of data and find outliers is something even the best human managers might miss, because we're often too busy to look at every line item every day. Ultimately, AI for data analysis helps MSMEs move from gut-feel decisions to data-driven decisions. Instead of guessing which product line is most profitable, the data (perhaps via a dashboard) can tell you. Instead of reacting when cash is almost gone, you get early warnings of trouble. The impact can be substantial – a Deloitte study found that small businesses using AI in decision-making saw an 18–24% improvement in ROI within the first year. When your decisions are backed by facts and forward-looking insights, you're effectively managing your business with the kind of foresight that large enterprises have – but at a fraction of the cost.

Workflow Automation in MSMEs

- **Finance & Accounts:** Before: Your accounts team might be manually entering every supplier invoice into Tally or an Excel sheet, then manually checking for errors or GST compliance. After: Using a simple OCR (optical character recognition) tool, you can scan invoices and automatically capture fields like vendor name, amount, GST number, etc., into your system. The software can flag if an invoice amount doesn't match a purchase order or if GST credit is claimed twice. Approval workflows can be automated too – for example, any expense above ₹50,000 can automatically notify the owner or CFO for one-click approval in a mobile app. Automation here means faster invoice processing, fewer data entry mistakes, and real-time visibility. Instead of waiting till month-end to see expenses, the boss can see "invoices waiting for approval" daily on her phone. Time saved is significant – one MSME reported their accounting staff used to spend two days reconciling payments and chasing missing bills; after automating reminders and using software to match bank entries with invoices, those two days have been reclaimed for more important analysis. As per a NASSCOM study, adopting AI-based automation helped small businesses cut overall operating expenses by about 20–30% on average, and finance/admin tasks are a big part of those savings.

- **HR & Admin:** Before: For a small organization, HR tasks like leave tracking or responding to employees' queries about policies can be a nuisance. Someone from HR (or often, just a senior manager doubling as HR) might be manually updating an attendance register, or answering the same question – "How many vacation days do I have left?" – multiple times a year. After: Workflow automation can handle these mundanely. There are lightweight HR management tools (some even free for small teams) where employees can apply for leave online, which then pings their manager for approval automatically and updates a leave balance. No paper forms, no manual summary at year-end. Chatbot assistants can answer common HR questions: "What's our travel reimbursement rate?" or "Is Diwali a holiday for us?" – the bot can instantly reply with the relevant policy snippet. For administrative approvals (like requesting a new laptop or permission to spend on a client dinner), you can set up a simple form that routes to the right approver's email and even sends reminders if it's not addressed in 2 days. The result is a smoother employee experience – things happen faster and with less confusion. And the HR person (if you have one) or the office manager is freed up to focus on hiring good people rather than pushing paperwork.

- **Operations & Supply Chain:** Before: Consider the workflow of purchasing raw materials or managing stock in a small manufacturing unit. Without automation, you rely on a supervisor's memory or a daily manual stock tally to know when to reorder. Purchase requisitions might be verbal or via emails, leading to delays or forgotten requests. After: Even basic automation can have a big impact here. For instance, you can set threshold alerts – if the stock of a key item falls below 100 units, the system automatically emails the purchase team or creates a draft purchase order. This way, you prevent stockouts proactively. Approvals for purchase can be streamlined: a digital form where the requester selects items needed, which then goes to the manager's phone for approval. Tracking orders with suppliers can be automated too – one MSME set up a system where the moment a supplier sends a dispatch email with a tracking number, that info is parsed and updated in their production schedule (so sales guys can see "material arriving by Friday" without chasing anyone). In the logistics side, low-cost IoT devices (like GPS trackers on trucks, or simple barcode scans) can feed data into an AI system that predicts if a delivery will be late. Before vs after, the difference is that managers spend less time firefighting (because the system already alerted them to a potential delay or shortage) and more time optimizing. A 2023 BCG study noted that Indian MSMEs using AI in supply chain management saw up to 40% reduction in excess inventory and 15% improvement in on-time delivery after adopting these tools – essentially by automating demand forecasts and inventory triggers.



- **Sales & Customer Relationship Management (CRM):** Before: Your sales team (even if that's just you and one more person) might be handling leads in an ad-hoc way – emails in an inbox, business cards from a trade show in a drawer, follow-ups when you remember. Customer service requests similarly might be handled via personal phone calls or scattered WhatsApp messages. After: A simple CRM system (there are several inexpensive ones aimed at small businesses) can centralize this. But beyond just a database, AI can make it smarter: it can auto-log interactions (some systems connect with your phone or email to automatically record that "you called Client X on Tuesday" so you don't have to log it), it can score leads (e.g., highlighting that a lead who visited your pricing page twice is more likely to convert, prompting you to call them), and set follow-up reminders ("It's been 10 days since you sent a proposal to Client Y – schedule a follow-up"). On the customer support side, AI can analyze incoming emails or chats for sentiment – an email in all caps with "angry" language could be flagged as urgent, ensuring you call that client immediately to resolve their issue before it escalates. Essentially, workflow automation in sales ensures no potential deal or customer complaint falls through the cracks. The effect is better revenue and happier customers. Think of it this way: before, a lead might go cold because you forgot to follow up; after, the system's nudging ensures timely follow-ups, which means more sales closed. No wonder even small sales teams are embracing these tools – it's like having a personal assistant who never forgets.

Across all these functions, the pattern is clear: AI and automation take over repetitive, high-volume tasks (data entry, routine checks, simple communications) which humans often find tedious and error-prone. The "after" scenario is not just about cost saving (though saving a few salaries worth of time or avoiding mistakes that cost money is important), it's also about speed and quality. Approvals happen in hours instead of days. Errors are caught automatically instead of being discovered in audits months later. And employees are happier because they can focus on more meaningful work – a finance officer can analyze profitability instead of stamping invoices all day, a store manager can talk to customers rather than just filling forms. It's a classic win-win: efficiency goes up, and so does work satisfaction.

Industry-Specific Examples

- **Manufacturing:** For small manufacturers, predictive maintenance is a game changer. Instead of waiting for a machine to break down (and losing production time), AI can analyze vibration or temperature sensor data to predict failures in advance. For example, a small auto parts factory installed an AI-based sensor system on its molding machines; it learned the normal vibration patterns and now alerts the owner's phone if any machine

shows unusual patterns that precede a breakdown. This allowed them to schedule maintenance over the weekend, avoiding unplanned halts. Another area is quality control – AI vision systems can now inspect products using cameras. Even a simple webcam with the right software can detect defects on a production line far more reliably than a tired human eye. In fact, AI-driven visual inspection can be so effective that studies show defect rates can be cut by up to 99% in some cases using such technology. Imagine a weaving unit that uses an AI camera to spot fabric defects: the system beeps to remove a flawed roll before it's sent out, virtually eliminating customer complaints about quality. These technologies, once costly, are now available as subscription services or low-cost devices, making them feasible for MSMEs.

- **Services:** In service industries (like clinics, consultancies, small BPOs, etc.), it's all about scheduling and information processing. Consider a small healthcare clinic. They started using an AI-based appointment system that lets patients book via WhatsApp. The system sends automated reminders to reduce no-shows and even optimizes the schedule by suggesting slots to fill cancellations. Patients are happier because they get quick responses and don't wait on hold. The clinic staff are less stressed because the schedule is smoother. Another example: a tax consultancy (MSME) that deals with piles of documents every season. They adopted an AI tool to automatically categorize and summarize documents – it reads PDFs of bank statements or invoices and highlights key info. What used to take an intern an hour per client, the AI does in minutes, letting the consultants focus on advising clients rather than extracting data. Service businesses also benefit from AI sentiment analysis on feedback – a hotel owner with 3 small properties uses an AI service to scan all online reviews and social media mentions of his hotels, giving him a daily summary: what guests liked, what they complained about.

This kind of insight (knowing that "guests find check-in slow" without having to read hundreds of reviews) allows small service providers to improve quality continuously. The common theme is better customer experience with less manual effort.

- **Retail/Distribution:** For those in trading, retail, or distribution, demand forecasting and inventory optimization are vital. A small electronics distributor integrated an AI forecasting tool with their sales data – it predicted which items would see higher demand in the coming month (based on trends and even local festival calendars). This MSME managed to increase sales by always stocking what customers wanted, and simultaneously reduced excess inventory by 40% because they weren't overstocking slow-moving items. In a retail context, personalization is key – even a small online store can use AI recommendation engines (often available as plugins for platforms like Shopify or Magento) to suggest related products to shoppers ("Customers who bought this also bought…"). These engines can increase average order value noticeably. And let's not forget on-time delivery – a lot of small businesses are using AI route optimization (some delivery apps offer this built-in) to ensure their deliveries cover the best routes, saving fuel and time. A food distribution MSME reported that by using an app that optimized driver routes, they could do 15% more deliveries per day with the same fleet, and customers got their orders sooner. In essence, AI helps level the playing field – a small retailer can now implement sophisticated techniques (like data-driven inventory and personalized marketing) that were once the domain of giant companies with big analytics teams.

These examples show that whatever your industry – be it a manufacturing workshop, a service-oriented firm, or a trading business – there are targeted AI and automation solutions available. Many of these come in the form of affordable SaaS (Software-as-a-Service) offerings or even free/open-source tools. The key is to start with a specific pain point in your industry and pilot a solution. If you're in manufacturing, maybe start with one production line's quality check. If you're in hospitality, try an AI chatbot for reservation queries. Real-world success stories are emerging every day, and MSMEs that experiment early stand to gain a competitive edge.

Tool Landscape: From No-Code to Enterprise Solutions

When it comes to implementing AI and automation, one size does not fit all. The good news is there's a rich landscape of tools catering to different skill levels and budgets. Here's a simple breakdown:

- **No-Code/Low-Code Platforms:** These are ideal for MSMEs who don't have in-house programmers. No-code tools let you create simple apps or automated workflows through visual interfaces. For example, using a service like Zapier or Microsoft Power Automate, a business user can set up something like "Whenever a new inquiry comes in via Google Form, send an automatic email reply and add the details to an Excel sheet." It's all drag-and-drop or form-based configuration. Low-code platforms are similar but allow a bit of scripting for flexibility. The big advantage is you can tailor small automations yourself without waiting for an IT project. Many of these platforms have free tiers or low monthly costs. They are a great starting point to dip your toes into automation – say, automate data transfer between your systems or create a simple chatbot without coding.

- **Ready-Made SaaS Tools for MSMEs:** There is now a SaaS (Software as a Service) product for almost every common MSME need, often with AI built-in. Some examples: customer support chatbots (with Indian language support) that you can subscribe to for a few thousand rupees a month, CRM systems like Zoho, Freshsales, or HubSpot that offer AI features to score leads or log calls, invoicing software that automatically reads receipts and prepares GST filings, or "RPA-lite" tools that let you record and automate repetitive computer tasks (like clicking through a government procurement portal to download forms every day). The benefit here is speed – you don't have to build anything, just configure and start using. When evaluating these, look for those specifically marketed to small businesses or MSMEs – they'll tend to be simpler and cheaper, without the excess complexity needed for a Fortune 500. For instance, an MSME could use a tool like KiSSFLOW or Oracle's SME suite which includes easy automation flows, rather than implementing a huge enterprise system.

- **Integration with Existing Systems:** A practical consideration is how new AI tools will work with what you already use. If your accounts are on Tally or your manufacturing process on SAP or your contacts in Excel, you want tools that can connect. Many modern software tools have what's called APIs or built-in connectors. If not, you might use a middleware (like a connector service) to bridge them. For example, you can connect your website form to your Tally accounting using a connector so that a new customer query automatically creates a ledger entry – it sounds complex but many providers have pre-built "bridges" for common software. When exploring AI solutions, check if they mention compatibility with your systems – e.g., "Works with Tally", "Slack integration available", "Import from Excel" etc. This can save a lot of headache.

- **Enterprise-Grade vs. Lightweight Solutions:** Be aware that many big tech companies offer AI platforms that sound exciting (like IBM's Watson, or Google's various AI services), but these might be overkill for a 50-person firm. Often, you're better off with a smaller, focused tool. That said, some enterprise tools have SMB packages or cloud versions which are pay-per-use. If you have a bit of IT support or ambition, you can even use open-source AI libraries (like running a Python script for data analysis) – but that's optional. The bottom line is: start with simpler tools and only graduate to more complex ones if you truly outgrow the basics.

So how do you choose the right tool? Keep in mind a few simple selection criteria before investing time or money: - Ease of Use: The tool should be usable by your team. A slightly less powerful tool that your staff actually adopts is better than a super-sophisticated system that no one uses. Look for intuitive interfaces and good onboarding support. - Cost: Evaluate the total cost – not just subscription, but setup or training costs. Many AI tools have a low entry price but tiered pricing as you scale. Make sure it fits your budget now and in the near future. - Integration: As noted, check that the tool plays well with your existing software or has an easy way to import/export data. Data stuck in silos isn't very useful.

Data Security: If you're putting business data into a cloud tool, ensure the vendor has proper security (encryption, compliance with standards). Read reviews or ask for security features. This is especially critical if you deal with sensitive customer data. - Support and Community: A reliable support team or at least an online community can be a lifesaver when you hit a snag. Opt for tools that offer responsive customer support (many SME-focused tools do hand-holding during onboarding) or have plenty of documentation/tutorials.

By evaluating tools on these criteria, MSMEs can avoid shiny-but-impractical solutions. For example, a small manufacturer might find that a no-code tool to automate purchase order emails is far more effective in practice than an expensive AI planning software that nobody fully understands. Start small, choose tools that solve your immediate pain points, and ensure they align with your team's capabilities.

Data, Privacy, and Governance

Introducing AI into your business is not just a tech project – it comes with responsibilities around data and processes. There's a popular saying: "garbage in, garbage out." AI is only as good as the data you feed it. For MSMEs beginning their digital journey, focusing on data quality is crucial. This means if you want accurate analysis, you need to maintain consistent records (be it sales, inventory, or HR data). For instance, if half your sales team logs client industry on each lead and the other half leaves it blank, an AI trying to find which industries to target will stumble. So, part of your AI plan should be standardizing data entry and cleaning up existing data – it might be boring, but it pays off in better AI results.

Privacy and consent are equally important. Small businesses often handle personal data – whether it's customer phone numbers, email IDs, or perhaps even Aadhaar numbers for KYC if you're a financial service provider. If you're using an AI tool that processes personal data (like an AI email responder that scans customer emails), you must ensure you're not violating privacy laws or customer trust. Some guidelines: inform customers if an AI is being used (for example, a disclaimer that "You are chatting with an AI assistant" on your website chat), make sure you have permission to use their data in whatever tool, and avoid feeding sensitive personal data into third-party AI tools unless necessary. Remember, if you're working with larger clients or government projects, they might have strict data handling rules – e.g., a PSU might require that data about their project should not be processed on foreign servers. Choose AI providers that allow options like India data centers or on-premise deployment if needed.

Then there's governance – basically, managing AI/automation use internally so it stays under control. Even a simple workflow automation can have unintended consequences if not monitored.

Say you automate sending reminders to clients for payments. If something goes wrong and the system spams a client with 10 messages instead of one, it can hurt your reputation. Governance steps for MSMEs need not be heavy: just define who can set up or change an automation (you don't want every employee creating automated email rules without oversight), keep a log of what automations are running (so you know, for example, that there is a bot sending WhatsApp replies – and who is maintaining it), and have an override or manual check for critical decisions. For instance, if an AI tool flags a transaction as fraudulent, have a human review it before action is taken.

Data security falls under governance too. Ensure backups are in place – if you automate invoice processing, don't let the only copy of scanned invoices sit in one system; back them up to another drive or cloud. Regularly update passwords and access for your tools (particularly if an employee leaves, make sure their access to the AI dashboard is removed). Logging and monitoring are your friends: many AI tools will keep logs of what they did – check them occasionally to catch any weird behavior. Regular reviews of automated processes can verify they're still doing what you intend as business conditions change.

One more aspect is compliance with regulations like the upcoming data protection laws in India (or GDPR if you deal with EU clients). Even as a small business, you should treat customer data with care – avoid uploading any personally identifiable info to random AI services without checking their privacy policy. Many AI providers offer enterprise-grade security features even for small users now, such as data encryption and compliance assurances – take advantage of that.

In summary, treat your business data as an asset. Keep it clean, secure, and use it responsibly. AI can amplify mistakes if you're not careful – for example, an AI could accidentally send a confidential report to the wrong person if it's not properly governed. But with some sensible precautions (documenting processes, controlling access, and monitoring outputs), you can reap AI's benefits while minimizing risks. Think of it as setting some ground rules before letting a very smart assistant into your workflow.

Change Management & Upskilling

When you introduce AI and automation, it's not just a technology change – it's a people change.

For many employees, the idea of "AI" can be intimidating. Will a bot replace their job? Will they be able to learn the new tools? As an MSME leader, you need to proactively manage this change and foster a culture that embraces these new assistants rather than fears them.

First, involve your team from day one. Identify the people who run the current processes (the purchase manager, the accounts executive, the customer support rep) and include them in discussions about automation. Ask them where the bottlenecks are – they might tell you that making a weekly MIS report is a pain, which could be solved by a simple automation. If they feel heard and see that automation is coming to help them, not judge them, they'll be more cooperative. For instance, if you plan to implement a chatbot, involve the customer support rep in training the chatbot – have them provide the most common questions and best answers. This not only makes the bot better, it also makes the employee feel like a key player (which they are).

Start with pilot projects and gather feedback. Instead of a big-bang "everything changes today" approach, do a trial for a few weeks. Maybe try the new workflow automation in one department or with one client. Encourage the team to note what they like and what frustrates them about the new system. Then actually use that feedback to tweak the setup. People support what they help create – if your staff sees their feedback leading to adjustments (like "the report should exclude cancelled orders, we fixed that now"), they'll trust the new tools more.

Invest in basic training and upskilling, but keep it practical. Your employees don't need to become AI scientists, but they might need to learn how to use an AI-powered tool effectively. Provide short, focused training sessions or tutorials. For example, if you roll out an AI-based analytics dashboard, have a session on "how to read the new dashboard and get insights" rather than dumping a link on employees with no guidance. If you deploy a chatbot, train the team on when to let the bot handle things and when to step in. You might also train them in creating effective prompts – for instance, a content writer in your team could learn how to use a tool like ChatGPT to draft marketing copy (with the skill being how to ask the right prompt to get a good result). An important area of upskilling is data literacy – helping staff understand data trends, basics of how AI makes decisions (to demystify it), and how to interpret outputs.

Keep in mind that at present, the digital skill gap is still large – only about 7% of India's MSME workforce has formal digital training. This means many will need hand-holding. But the flip side is, once trained, your workforce becomes much more capable and confident, which is a competitive advantage for you.

Another aspect of change management is addressing the "job loss" fear. Be honest and transparent that the goal of AI is to assist people, not replace them. You can highlight that offloading routine work will free them for more important tasks. A real example: a small accounting firm that automated data entry assured their accountants that no one would be laid off – instead, they'd focus on financial analysis and advisory (higher value work). They even tied a bit of bonus to how well employees adopt the new system, to show that the company values their transition. Over time, as employees see the drudgery reduce, they usually come around. It's very important to communicate success stories internally – e.g., "Since we introduced the automated customer FAQ, our support team has been able to respond to complex queries 30% faster – great job team for making it work!" Celebrate the positives so that AI is seen as a team win.

Lastly, encourage a culture of continuous learning. AI tools and best practices will evolve, so make learning part of work. This could be as simple as having one team member attend a free webinar on new AI trends each month and share a couple of insights with everyone. Or setting up a small internal forum (maybe a WhatsApp group) where people can drop tips like "Hey, I found a shortcut in the new software that saves time." When people feel they are growing their skills and not being left behind, they will embrace change rather than resist it.

Step-by-Step Implementation Road-map

Embarking on AI and automation can be overwhelming, so it's best to break it into clear steps. Here's a straightforward roadmap any MSME can follow:

1. Identify 2–3 Pain Points: Start by picking a few high-volume, repetitive or error-prone tasks in your operation. These are your "low-hanging fruits" for automation. It could be data entry in accounts, first-level customer inquiry responses, inventory reordering, or report generation. Choose areas that frequently cause delays or quality issues, or simply eat up a lot of employee hours.

2. Map the Current Process & Set a Baseline: For each chosen task, document how it's done today – who does what, how long it takes, how often mistakes happen, etc. This doesn't need a fancy flowchart; even a simple written step-by-step is fine. Importantly, note the baseline metrics: e.g., "It takes 3 days to compile the monthly sales report" or "We get 50 support calls a week, and it takes on average 4 hours to resolve each." These will help you measure improvement after automation.

3. Explore Tool Options (2–3 each): Research a couple of automation or AI tools that could address each pain point. Look for low-cost or freemium solutions first. For instance, if the pain point is managing social media queries, options might be a free chatbot from Facebook or a low-cost social media management tool that has automation. If invoice processing is the issue, look into an OCR invoice scanner. The idea is to find a shortlist of potential solutions – use the criteria from the earlier section (cost, ease, integration, etc.) to guide you. At this stage, also talk to peers or consult tech forums – other MSME owners might recommend something that worked for them.

4. Run a 4–8 Week Pilot: Don't jump into full implementation. Pick one of the tools (or one per use-case) and run a pilot for a defined period, say a month or two. During the pilot, use the tool in real work but perhaps in parallel with your old process initially (to ensure nothing breaks). Set success metrics beforehand – for example, "pilot success = customer response time cut from 4 hours to 1 hour," or "inventory stockouts reduced to zero this month." Make sure the team using the tool knows it's a trial and their feedback is crucial. Keep the pilot scope limited (like one department, or one type of transaction) to manage risk.

5. Review Results and Refine: At the end of the pilot, assess the metrics versus your baseline. Did the automation meet the goals? Sometimes you'll find it helped, but not as much as expected – that's okay. Gather qualitative feedback too: maybe the customer service staff say the new chatbot answered 80% of questions but struggled with 20%. With this insight, refine the setup or consider trying the second option from your shortlist if the first one wasn't great.

If the pilot did deliver good results (say you saved a lot of time), plan the next steps: scaling it to more users, or integrating it deeper (e.g., fully replacing the old process).

6. Scale Up and Establish Governance: Once confident, roll out the solution to all relevant parts of your business. As you scale, set up simple governance – assign an owner for the tool (who ensures it keeps running and is updated), schedule periodic reviews (maybe a 30-minute monthly check on "is the tool still delivering, any issues?"), and document any changes you make. Also, if the pilot was in one area, now consider adjacent processes that could benefit. For instance, after automating invoice entry, maybe next scale to purchase orders or payroll. Essentially, build on your success gradually.

This step-by-step approach ensures you start small, learn and adjust, and then scale – reducing risk and investment. It also creates internal champions; the people involved in pilots become your experts who can train others. One MSME following a similar roadmap shared that by step 4 they discovered the first tool they tried for task scheduling was too clunky, so they switched to another in step 5, which then became a hit in step 6 across the company. The iterative approach saved them from a huge sunk cost in the wrong solution.

Risks, Limitations, and How to Avoid Pitfalls

While AI and automation offer many benefits, it's wise to go in with eyes open about the potential pitfalls. Here are some common risks and how to mitigate them:

- **Over-Promising Vendors:** Not every shiny AI tool will deliver what salespeople claim. There's a lot of hype, and some vendors might promise "magic" (e.g., "99% accuracy guaranteed!"). Avoiding the pitfall: Do your due diligence. Ask for a demo or a trial period. Seek references – do they have other MSME clients you can speak to? Start with a pilot (as described) before a full purchase. Essentially, trust but verify. If a vendor is evasive about letting you test or about clarifying what exactly the AI does, that's a red flag.
- **Hidden Costs and Subscription Creep:** Many tools start cheap but additional features or usage can raise the cost. You might start with one tool, then add another, and suddenly you have multiple subscriptions eating your budget (often called "subscription creep"). Avoiding the pitfall: Keep track of direct and indirect costs. Negotiate fixed pricing where possible or set usage caps. Periodically audit what you're paying for – maybe that fancy analytics module isn't being used, and you can downgrade. Also, consolidate tools if possible (some platforms do multiple things, which might be more cost-effective than many single-point solutions).
- **Poor Data Security or Backup Practices:** If not careful, you might automate yourself into a corner. For instance, if a process becomes fully automated and no one monitors it, you might not notice if data is not being backed up or if a silent error is creeping in. Also, using cloud tools without checking security can expose you to data breaches. Avoiding the pitfall: Implement basic IT hygiene – regular backups (automation can help here too, by the way, by auto-backing up cloud data to a local drive weekly), access controls (ensure ex-employees or interns are removed from systems promptly), and using trusted services (check if the provider has security certifications like ISO 27001 or follows GDPR, etc.). Also, have a manual override plan: if your AI tool went down for a day, do employees know how to carry on work manually temporarily? Maintaining that "plan B" can save the day in emergencies.
- **Unrealistic Expectations:** Some businesses think adopting AI will solve all problems overnight – that's rarely the case. If leadership expects a magical transformation in a month, they will be disappointed and could sour on genuinely useful technology. Avoiding the pitfall: Set realistic, incremental goals. Recognize that AI is not a plug-and-play brain – it needs to learn and often needs tweaking. Measure success in specific areas, not broadly ("reduce order processing time by 30%" rather than "improve customer satisfaction instantly"). Manage stakeholder expectations by communicating that initial results might be modest but will improve. And remember, AI is a tool, not a strategy – if a process is fundamentally broken, fix the process; AI on top of a broken process won't help.

Another risk worth mentioning is employee pushback or misuse – if not guided, people might try to game the new system or avoid using it. Address this by involving them and perhaps putting in checks (like if the new timesheet system is automated, ensure everyone knows their inputs are still monitored for accuracy).

By anticipating these pitfalls, you can take simple steps to avoid them. Think of it like driving a car: you know the risks (accidents, breakdowns) so you take precautions (seatbelts, maintenance). Similarly, with AI in your business, a little foresight and governance goes a long way to ensure a smooth ride.

Conclusion: From Experiments to Competitive Advantage

To wrap up, let's recap the core benefits an MSME can gain from embracing AI and automation:

- **Time Savings and Efficiency:** Routine processes happen faster (reports in seconds, not days; approvals in hours, not weeks), freeing employee time for more value-added work.
- **Error Reduction and Quality Improvement:** Automated data entry and AI checks mean fewer mistakes – invoices don't go unpaid due to human error, and products have fewer defects, leading to more consistency and trust.
- **Better Decision Making:** With AI analyzing data and making predictions, you get insights that help you make informed decisions (like what to stock, whom to target, where to cut costs) rather than relying purely on gut feel.
- **Enhanced Customer Satisfaction:** Faster responses, 24/7 support, and personalized engagement (recommendations, follow-ups) make your customers and big clients happier, strengthening your relationships and reputation.
- **Scalability and Growth:** Automation lets you handle more business without a linear increase in headcount. It sets the stage for scaling up – you can take on that extra contract or expand to new markets because your processes can handle more volume.

In today's business environment, adopting these technologies isn't just about internal efficiency – it's becoming a market expectation. .

Large customers like PSUs, MNCs, and government departments are increasingly looking for suppliers who are digitally savvy and reliable. An AI-enabled MSME stands out because it can provide timely data, adapt quickly, and integrate smoothly into digital supply chains. For example, some government tenders now prefer vendors who can comply with electronic data interchange or automated tracking updates. If you as an MSME have those capabilities (thanks to your automation efforts), you become a preferred partner. Essentially, being "AI-ready" or even "AI-augmented" is turning into a competitive advantage. It signals that your business is forward-looking and efficient, which can tip the scales in winning contracts or clients.

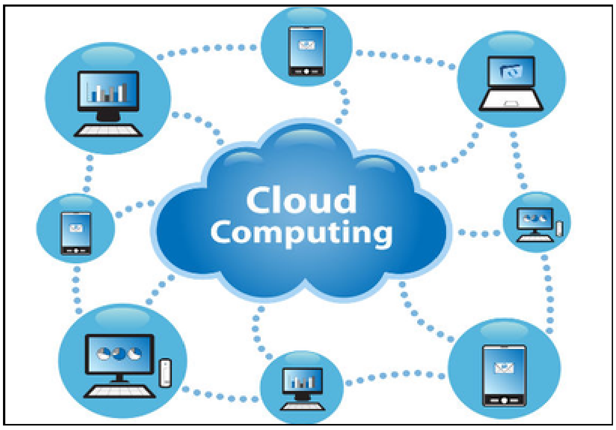
The journey from experimenting with a small automation to fully leveraging AI across your business is a gradual one – but it's a journey worth starting. Think of it as adding layer upon layer of improvement. Each little bot or tool you deploy takes away some friction and adds to your capabilities. Over a couple of years, these small gains compound into a significantly smarter and more agile organization.

So, where should you begin? My advice: start with one small automation this quarter. Pick one process that annoys you the most and try an AI or automation solution for it. It could be as simple as automating your payment due reminders or setting up a bot to collect customer feedback. Use the outcome to learn and to build confidence. Success with one project will energize you and your team to tackle the next. In a year's time, you might find that AI and automation have moved from being experiments to being an integral part of how you work – quietly and efficiently boosting your business every day. In the dynamic marketplace ahead, that could make all the difference between those who lag and those who leap forward. The tools are within your reach – it's time to grab them and innovate.

CMA Madhuri Kashyap

Treasurer, Northern India Regional Council,
The Institute of Cost Accountants of India
Former President, International Navodaya Chamber of Commerce

Cloud Computing: The Benefits and Risks of Migrating Operations to the Cloud (Storage, CRM, Accounting)



Introduction

Why Cloud is at the Centre of Digital Transformation

On a rainy Monday, the IT team of an organisation relying on outdated on-premise servers is scrambling – their local server in the office just crashed again, knocking out the inventory software and email system. They face issues with scalability (adding new users or storage is a major project), supporting remote work is clunky, and even security updates get missed because the lone IT chap is overloaded. This scenario is common for many organisations that still depend entirely on on-site IT.

Enter "the cloud." Simply put, cloud computing means using computing services over the internet – from data storage to software applications – hosted in data centers owned by providers like Amazon, Microsoft, or Google (or even government-owned clouds). Instead of running software on your own office servers or PCs, you access it as a service on the cloud provider's infrastructure. For example, if you use Gmail or Office 365, you're using cloud-based software as a service (SaaS). If you rent virtual machines or storage from Amazon Web Services, that's cloud infrastructure (IaaS). The cloud is essentially someone else's computer (or thousands of them), which you use on-demand.

Why is everyone talking about moving to the cloud now? A few key statistics tell the story. Global cloud adoption has exploded in recent years. In 2025, the global cloud computing market reached about $913 billion, up from just $156 billion in 2020– a nearly sixfold increase in five years. Today, over 90% of organizations worldwide use cloud services in some form, whether for email, data backup, or entire business applications. Even traditionally cautious sectors are making the shift. In fact, a survey found that about 60% of organizations now run more than half of their workloads in the cloud, up from 39% in 2022.

This trend accelerated during the pandemic when remote work became critical. Businesses that had their systems "in the cloud" could transition to work-from-home far more smoothly than those that had everything tied to an office server.

India too is riding this cloud wave. The Indian government's digital initiatives and affordable internet have spurred cloud adoption among companies and public sector units alike. The Indian cloud market was around $18 billion in 2024 and is projected to reach about $76 billion by 2030, reflecting rapid adoption even among traditional sectors. Cloud services like email, video conferencing, and digital procurement platforms (e.g., the Government e-Marketplace) have become essential infrastructure. One report forecasted that India's e-commerce and other digital services would push cloud usage to INR17.7 trillion (≈$211 billion) by 2025 in market value.

But what exactly is "the cloud" beyond the buzzword, and how can it help (or in some cases, challenge) your operations? Let's break it down in plain language.

Basics of Cloud Computing (Without Heavy Jargon)

Cloud services come in different flavors, usually described as "X as a Service." The three main types are: - Infrastructure as a Service (IaaS): This is the most basic form – renting raw computing resources. Instead of buying servers, you rent virtual servers, storage, or networking from a provider. You manage the operating system and applications, but the hardware is in the provider's data center. Example: hosting your company's website on an Amazon EC2 virtual machine or storing backups on Azure Blob Storage. Platform as a Service (PaaS): Here, the cloud provides a platform (a managed environment) for developing and running applications without worrying about the underlying servers.

Think of it as a pre-set kitchen where you can cook your dish without having to build the kitchen. Example: Google App Engine or Microsoft Azure App Service where you can deploy your app and the platform handles the servers, scaling, and runtime. - Software as a Service (SaaS): This is fully finished software delivered over the internet, which you use through a browser or app. You don't manage anything infrastructure-wise – you just use the software. Examples are everywhere: Gmail for email, Salesforce for customer relationship management, Google Drive or Dropbox for storage, Zoho Books for accounting, Microsoft Teams for collaboration, etc. Most SaaS is on a subscription (monthly/annual per user).

In simpler terms, IaaS is like leasing a plot of land (with power and water hookups) where you can build what you want, PaaS is like leasing a fully equipped workshop where you just bring your ideas and materials, and SaaS is like renting a finished office that's ready to use. Many managers might be using cloud services without realizing – if your company uses a web-based payroll service or a cloud CRM, you've already embraced SaaS.

Another concept: public vs private vs hybrid cloud. - Public cloud means services offered by third-party providers to many customers over the internet (publicly accessible). Examples: AWS, Microsoft Azure, Google Cloud – they operate huge shared data centers. - Private cloud means a cloud infrastructure dedicated to one organization (it could be on-premise or hosted, but not shared with others). Large enterprises or government agencies with extra security needs sometimes maintain private clouds – basically their own mini-AWS for internal use. - Hybrid cloud is a mix of both: some workloads run on public cloud, some on a private cloud or on-premises, with integration between them. For instance, a company might keep sensitive data on a private cloud (or on-prem) while using public cloud for less sensitive applications, and the two environments talk to each other.

To keep things simple: most MSMEs and even many large companies find public cloud solutions the most economical and flexible for general needs, whereas private clouds are considered when there are stringent regulatory or performance needs that demand dedicated infrastructure.

You're likely already familiar with some cloud-based tools as an end user. If you use webmail (like Yahoo/Outlook.com), that's SaaS. If your team shares files on Google Drive or Microsoft OneDrive, you're leveraging cloud storage. HR portals, CRM systems, even many government e-procurement portals are cloud-based applications. The point is, cloud computing is not an alien concept reserved for tech giants – it's a continuum of services that ranges from basic to advanced, and many are plug-and-play for businesses of any size.

Benefits of Migrating to the Cloud

Migrating operations to the cloud can bring a host of benefits. Let's break down some of the biggest advantages with real-life flavor:

Cost and Flexibility

One of the most touted benefits of cloud is the pay-as-you-go model. Traditionally, if you wanted to run an ERP system, you'd need to invest upfront in expensive servers, storage, networking gear, plus pay for IT staff to maintain them. This is a capital expenditure – money paid up front regardless of actual usage. In the cloud, you can typically start with a small instance or a few user licenses and pay monthly only for what you use. Need more capacity during the festive season? You can scale up for those months, then scale down to reduce costs in off-peak times.

This flexibility can be a lifesaver for seasonal businesses or projects. For example, an e-commerce company might see 5x traffic during Diwali. In the old model, they'd have to buy enough servers to handle that peak (which sit idle most of the year). In the cloud model, they simply ramp up their cloud servers for a month (incurring higher fees for that period) and then dial them back down – overall cost is lower than owning idle hardware. No more huge upfront hardware investments that lock your capital.

Moreover, cloud eliminates many "hidden" costs of on-premise IT – electricity for running and cooling servers, physical space for a server room, hardware maintenance contracts, and replacement of aging equipment every 3-5 years. All that is handled by the provider, whose economies of scale make it cheaper. A study by Accenture found that moving workloads to the public cloud can reduce total cost of ownership by around 30–40% on average. And if your usage is low, the savings can be even more, since on-prem costs don't scale down when you're idle, but cloud costs do.

Speed and Innovation

In the cloud, deploying a new server or application can be done in minutes with a few clicks, as opposed to waiting weeks for procurement and setup of hardware.

This speed to deployment means companies can experiment and innovate faster. For instance, if your analytics team wants to try a new data visualization tool, in the cloud they could start a server and try it out this afternoon, and shut it down if it's not working out (costing perhaps a few hundred rupees). On-prem, that request might go into an IT queue, eventually leading to buying a new server or repurposing one (costing perhaps tens of thousands and taking days or weeks).

This agility extends to software development as well. Cloud platforms provide ready-made environments to develop and test new applications quickly. Many businesses credit cloud adoption for enabling a more experimental, innovative culture – it's low risk to try new ideas when infrastructure is cheap and on-demand. Additionally, cloud providers are constantly rolling out new services (AI, machine learning, IoT platforms, etc.) which you can tap into without having to build that capability from scratch. In a sense, moving to cloud is like moving to a city with an amazing public infrastructure – you suddenly have access to world-class roads, power, and services that you can utilize to build whatever you want more quickly.

Another major advantage is the cloud's built-in reliability. Reputable cloud providers have data centers distributed across multiple locations and include features like data replication. If one server fails, your application automatically shifts to another; if an entire data center goes down (due to a power outage or natural disaster), systems can failover to a different region. Achieving this level of disaster recovery and redundancy on-premise is extremely expensive – typically only very large enterprises set up multiple geographically separated data centers for DR. In the cloud, even small businesses can afford to keep backups in a different region or use multi-zone architectures, often with a few configuration settings.

Reliability and Business Continuity

For example, a fintech startup in India runs their core application on a cloud platform across two regions – if one region has an outage (which is rare but possible), the system seamlessly falls back to the other region. Their customers don't experience downtime, whereas if they had one on-premises server, any failure would mean an immediate outage. Cloud providers also handle regular backups, hardware replacements, and maintenance behind the scenes.

Business continuity options that were once out of reach for MSMEs (like having a live secondary site) are now accessible pay-per-use on cloud. That said, you still have to architect correctly to use these features – simply putting something on a single cloud server isn't automatically foolproof – but the tools are there to achieve high reliability without owning duplicate infrastructure.

Collaboration and Remote Work

Cloud services enable anytime, anywhere access, which has become vital in the era of remote and hybrid work. When your data and applications are in the cloud, employees, vendors, and partners can securely access what they need from any location (with internet access and proper credentials). Contrast this with the old model where, say, your accounting software is installed on a PC in the office – if the team is working from home, they either can't use it or have to go through clunky VPNs into the office network.

Consider a scenario: a project team spread across Mumbai, Bengaluru, and a small town in Uttarakhand. If they use a cloud-based project management tool and store documents in a shared cloud drive, everyone sees the latest files and updates in real time, without emailing attachments back and forth. They can even collaborate simultaneously on documents via Google Docs or Office 365 – something impossible with files locked on one office PC. This not only improves productivity but also attracts talent – people can work for you without relocating, and you can continue operations during disruptions (like lockdowns or natural events) because your office is essentially virtual. It's no wonder that companies that had invested in cloud tools fared much better during the COVID-19 lockdowns.

To give a concrete example, a government department in India shifted its internal communications and document workflow to a cloud-based system as part of the Digital India push. They found that inter-office memo processing time dropped drastically, as files were no longer moving physically or stuck on one person's desk – everyone could access the digital file concurrently and approvals moved faster. Similarly, a lot of PSU vendors now submit bids and invoices through cloud portals.

The collaboration benefits of cloud are clear: a single source of truth for data that all authorized users can view or edit, from any device, often in real time, leading to fewer version mismatches and faster turnaround.

Finally, a quick note on a simple cost comparison to illustrate the benefit: Imagine you have a small CRM server on-premise that costs you ₹5 lakh in hardware every 5 years, plus ₹1 lakh/year in maintenance and electricity, etc. That's roughly ₹2 lakh per year cost averaged out. Now, moving that to a cloud VM might cost you, say, ₹10,000 per month (₹1.2 lakh/year). Already you're saving money. Plus, if you need to double capacity for 2 months, you pay maybe ₹20k for those months and then scale back – on-prem you would have to over-provision permanently to handle that peak. These rough numbers often pan out in favor of cloud, especially when you account for intangible benefits like less downtime or the value of quicker deployments. No wonder Deloitte found that SMBs leveraging cloud saw 21% higher profit and 26% faster growth than their peers– the cloud empowers efficiency and agility, which directly impact the bottom line.

Use Cases: Storage, CRM, Accounting and Beyond

Cloud computing isn't a one-size-fits-all; you can choose specific areas of your operations to move to the cloud based on the benefits you seek. Let's explore a few key use cases and examples:

- **Storage & Backup:** One of the simplest ways to start with cloud is moving data storage and backups offsite. Instead of keeping all files on a local server or individual PCs (which could crash or get stolen), businesses use cloud storage services. This provides a central, searchable repository for documents accessible from anywhere. For example, a construction firm replaced their on-prem file server with Google Drive for Work – now engineers at sites and staff in the office always access the latest drawings and documents. Moreover, cloud storage often comes with versioning (so you can retrieve an older version of a file) and automatic backup features. You can set policies to back up critical systems to the cloud daily, mitigating the risk of data loss. Consider a CA firm that backs up client data to an encrypted cloud storage every night – even if their office systems fail, they can restore data from the cloud quickly and meet their compliance needs.
- And speaking of compliance: many cloud providers have certified data centers (for ISO, etc.), which can help meet regulatory requirements for data handling, as long as you configure things correctly.
- **CRM & Sales:** Cloud-based Customer Relationship Management (CRM) systems like Salesforce, Zoho CRM, or Microsoft Dynamics 365 have transformed how sales and service teams operate. Traditionally, a company might have an old contact management software on one office computer, or rely on Excel sheets. With a cloud CRM, your salespeople can log leads, update customer interactions, and track deals in a single system accessible from phone or laptop. Managers can get real-time dashboards of sales pipelines without having to compile reports manually. Moreover, these systems often integrate with email, calling, and marketing tools out of the box (since everything's in the cloud, integration is easier). A tangible benefit: imagine a service company where a customer calls support; with a cloud CRM, the support agent can see that customer's entire history (past tickets, purchase records) on one screen, because the CRM is integrated with other cloud apps. This means faster, more personalized service. Cloud CRMs also enable better collaboration – a salesperson can tag a colleague or set tasks in the CRM for follow-ups, and everyone sees updates instantly. And of course, being cloud-based, a salesperson on the road can update a lead status right after a meeting on their mobile, rather than waiting to "get back to office." The result is often higher sales efficiency and better customer experience.
- **Accounting & ERP:** Accounting was one of the earlier functions to go cloud in many SMEs – with services like QuickBooks Online, Xero, or India-specific solutions like Zoho Books and newer cloud-based Tally offerings. A cloud accounting system means your finance data is accessible to authorized users (the accountant, the CFO, even the CA/auditor via secure access) from anywhere. No more passing USB drives or worrying that the accounting PC might crash. It also eases compliance – many cloud accounting software can automatically calculate GST, generate e-invoices, or file returns directly by integrating with government portals. Real-time financial reporting becomes feasible – the boss can pull up today's sales or this quarter's P&L on their phone. For larger organizations using ERP (Enterprise Resource Planning) systems like SAP, the cloud is also making inroads. SAP's latest flagship (S/4HANA) is available in a cloud edition, which simplifies the notoriously heavy infrastructure needed for SAP. Companies that migrate ERP to cloud often cite benefits like easier multi-location access (all branches use one cloud ERP versus maintaining servers at each branch) and simpler updates (the provider handles updates).

One government enterprise portal, for instance, moved its procurement and inventory system to a cloud-based ERP module – this enabled their vendors (mostly MSMEs) to connect through the internet directly to the system for orders and invoice submissions, something that was clunky and VPN-based before. Real-time reporting, consolidation across units, and easier compliance (because the software stays up to date with tax rules) are big advantages of cloud-based finance systems.

Sector-Specific Examples:

- Public Sector/Citizen Services: Many government departments now use cloud-hosted portals to deliver services (like applying for licenses, paying taxes, etc.). Cloud allows these portals to handle huge user volumes (for instance, during a scheme application window) by scaling up automatically. It also ensures better uptime for critical public services. India's own MeghRaj Government Cloud initiative was set up to help departments launch digital services without each having to invest in separate data centers.
- Manufacturing/IoT: Cloud combined with IoT (Internet of Things) enables factories to monitor equipment in real-time. Sensors on machines send data to cloud analytics platforms which can trigger alerts or maintenance requests. For example, a small manufacturing company uses a cloud IoT service to gather temperature and vibration data from machines on the shop floor. If any reading goes beyond threshold, the service alerts managers on their phone. This prevents breakdowns and optimizes maintenance schedules. The heavy processing (analyzing thousands of data points for patterns) is done on cloud servers – the MSME didn't need to buy powerful computers for it, they just pay a usage fee.
- Retail and E-Commerce: Many retailers run their point-of-sale systems and inventory management on cloud-based solutions now. This means every sale in a store updates the central inventory instantly on the cloud, and management can see sales across all outlets in real time. During peak sales (like a festival sale), the cloud infrastructure can scale so the billing systems don't slow down. Also, adding a new store is easier – just connect to the cloud app, no local server setup. On the e-commerce side, obviously the entire business is digital – cloud hosting ensures that an online shop can handle surges in traffic when a product goes viral. For instance, an MSME that sells handicrafts online on its own site might use a cloud hosting service that automatically copes if, say, a celebrity tweet drives a 10x spike in visitors. Without cloud, that spike might crash an on-prem server.
- Healthcare: Clinics and hospitals are adopting cloud-based health record systems.
- A clinic using a cloud EMR (Electronic Medical Records) can allow patients to access reports via an app, doctors to update prescriptions digitally, and ensure data is backed up. During the pandemic, some telemedicine startups scaled rapidly via cloud video conferencing and consultation platforms, something that would've been very hard with only on-prem infrastructure.

These use cases show that cloud computing is incredibly flexible – it's not just for web startups, but for traditional businesses, service providers, and government alike. The key is to identify which parts of your operations can benefit most (cost reduction, flexibility, remote access) and consider a cloud solution for those. You don't have to move everything at once – many organizations start with one area (email or backup or a new app) and gradually expand.

Risks and Challenges of Cloud Adoption

It's not all sunshine in the cloud – there are legitimate concerns and challenges when migrating. Being candid about these helps in planning how to mitigate them. Let's discuss candidly:

Security and Privacy Concerns

Arguably the number one worry: "Is my data safe on the cloud?" When you put data on cloud servers, you are entrusting it to a third party. High-profile breaches or leaks can happen if things are misconfigured or if the provider is targeted. For small businesses, a concern is often sensitive customer data (like financial records, personal information) or intellectual property being stored off-premise. For example, consider a healthcare clinic moving patient records to a cloud app – they must ensure patient privacy is protected as per laws like the Data Protection Act or HIPAA (if dealing internationally). If the cloud database were compromised, those patient records could leak, which would be a serious breach of trust and compliance.

Another scenario is a multi-tenant environment (which is how public clouds work – many customers on shared hardware). While strict isolation exists virtually, some worry about co-location risks or potential cross-tenant vulnerabilities (though rare).

A related risk is human error – many cloud data leaks in recent years were due to misconfigured settings (like leaving a storage bucket publicly accessible by mistake). So, security in the cloud is doable, but it's different. You have to be vigilant in setting the right access controls and using encryption features. A survey indicated 95% of companies are concerned about cloud security – that shows it's a universal worry, not just yours.

Compliance and Data Localisation

Different industries and countries have regulations about where data can reside and how it must be handled. For example, EU's GDPR regulates personal data handling, and in India certain financial or government data might be required to stay within national borders. Using an international cloud could inadvertently violate these if you're not careful. For instance, a financial firm uploading customer KYC data to a cloud might need to ensure the provider stores it in India data centers to comply with RBI guidelines. Similarly, government departments often require community or government clouds where data is on Indian soil and perhaps in infrastructure vetted by the government. If an MSME supplies to a defense organization, they might be told not to put project data on foreign cloud servers due to sensitivity. So compliance is a big factor – before migrating, one must understand the regulations applicable and ensure the cloud provider can meet them (many offer region selection and even dedicated government cloud offerings now).

Data localisation is a hot topic – some sectors might mandate it (like payments data per RBI). The risk if ignored is legal trouble or losing business. The challenge is that not all cloud services had India presence until recently, but this is improving with major players opening Indian data centers. You can usually choose your data region in public clouds; make that choice wisely for sensitive data.

Vendor Lock-In

Moving to the cloud can sometimes feel like jumping from the frying pan to the fire in terms of dependence – instead of being stuck with old hardware, you might become too dependent on a single cloud vendor. Each cloud platform (AWS, Azure, GCP, etc.) has its own ecosystem of services. If you heavily use proprietary services (like AWS Lambda, Azure Cosmos DB, etc.), migrating away later could be difficult without significant rework, because those services might not have exact equivalents elsewhere. Companies fear scenarios like: you start with low costs on one platform, then a few years in, prices increase or service deteriorates, but you can't easily switch because your whole environment is tailored to that platform.

A related issue is if the vendor goes out of business or discontinues a service you rely on (more common with smaller SaaS startups or niche providers). Then you have to scramble for alternatives. The challenge is to avoid lock-in by design: use standard technologies where feasible, keep backups of your data in formats you control, and perhaps adopt a multi-cloud strategy for critical systems (though multi-cloud can increase complexity).

Some organizations mitigate lock-in by using containerized applications and open-source components that can run on any cloud infrastructure. However, this can sacrifice some of the convenience of using cloud-specific high-level services. There's a balance to be struck. Many CIOs adopt a "primary cloud with escape plan" approach – choose one cloud for most things but have contingency if needed (even if that contingency is bringing some systems back on-premise or to another cloud if absolutely required).

Cost Overruns and "Shadow IT"

While cost was listed as a benefit, it can also become a challenge. On cloud, it's easy to spin up resources – and equally easy to forget to turn them off. If not monitored, you might get surprise bills. For example, a development team in a company might deploy a test server and then forget about it, incurring charges for months. Additionally, with cloud, different departments might directly sign up for services (this is often called "shadow IT" when done without central IT governance). Finance might start using a cloud BI tool, marketing might use a SaaS for bulk emailing, etc., and the organization could end up with many subscriptions and redundant spending.

One concrete scenario: a startup found its cloud bills creeping up because developers had dozens of instances running and storage buckets accumulating logs. They realized they needed to implement cost monitoring tools and policies to shut down unused resources. A report on cloud challenges indicated managing costs is one of the biggest barriers to fully embracing cloud, for both enterprises and SMBs. Cloud bills being OPEX need active governance, similar to keeping utility bills in check.

Mitigation: Set budgets and alerts on your cloud account (all major clouds allow you to do this). Implement tagging of resources by project/department to track usage. Encourage a culture of "clean up after use" – e.g., schedule temporary servers to auto-delete after a period. And centralize visibility: maybe the IT lead or accountant reviews all cloud subscriptions quarterly to see if anything can be pruned or consolidated.

Skill Gaps

Your IT staff may be very proficient at managing physical servers or traditional software, but cloud requires a different skill set – understanding cloud architectures, automation (Infrastructure as Code), security configurations, etc. There can be a learning curve. Many organizations struggle initially because they try to apply on-prem thinking to cloud and either misconfigure things or miss out on cloud benefits. For example, an admin might set up a cloud VM and treat it like an on-prem server, logging in manually to maintain it, whereas the cloud way would be automating it and using managed services instead. The risk is underutilizing the potential of cloud or making mistakes that could cause outages or insecurity.

Investing in training or hiring cloud-savvy talent thus becomes necessary. Suppose a PSU's IT department shifts a major system to cloud – they might need to re-train system admins to manage cloud resources effectively, or bring in a cloud expert contractor for initial guidance. Not doing so can result in suboptimal setups or even incidents (e.g., someone accidentally exposing a database because they didn't understand the cloud firewall settings).

For small businesses without dedicated IT, this challenge often means using managed solutions or getting consulting help for setup. The good news is many cloud providers offer free training resources, and the community forums are rich with advice.

To make these risks feel real: imagine a small e-commerce business that rushed to cloud during a traffic surge. They migrated their database to a cloud service but didn't configure an access rule properly – a security breach happened, and they lost customer trust. Or a company that moved to cloud and saw bills double expectations because they kept old habits of oversizing servers. These stories underline that cloud adoption needs planning and new governance, not just tech changes.

Cloud Security Essentials – Shared Responsibility

When using cloud services, it's crucial to grasp the concept of the shared responsibility model. In essence, the cloud provider is responsible for securing the cloud infrastructure (the physical data centers, the servers, the networking, and foundational services), while the customer is responsible for securing what they put in the cloud (their data, user access, application configurations, etc.). A simple analogy: if you rent a vault in a bank's storage facility, the bank ensures the facility is secure (guards, locks on the building), but you must securely lock your own vault and manage who has the key.

For example, when using an AWS or Azure cloud server, Amazon/Microsoft will ensure that their data center has tight physical security, their hypervisor (which creates virtual machines) is secure against breaches, and so forth. But if you misconfigure your security groups (cloud firewall) to leave ports open, or use weak passwords, that part is on you. Many breaches in cloud environments happen because the customer didn't do their part – such as leaving an S3 storage bucket public or not securing API keys.

So what are some minimum security hygiene practices when on the cloud? - Identity and Access Management (IAM): Use the principle of least privilege. Create individual user accounts for people/services with only the permissions needed, rather than sharing one master login. Turn on multi-factor authentication (MFA) for cloud console access or any sensitive login – this adds a one-time code or app approval in addition to password, making it much harder for attackers. (Many breaches start with stolen credentials; MFA can thwart that.) Also, consider using centralized identity if possible (like linking logins to your business Microsoft/Google accounts) so that you have one place to disable access when someone leaves. - Encryption: Always enable encryption for data at rest and in transit if the service supports it (most do). For instance, ensure your cloud storage buckets have encryption turned on, and use HTTPS for any data moving in/out. This way, even if someone intercepts data or if a storage device is stolen (unlikely at a provider, but still), the information is unreadable. Many cloud services make this a checkbox or default – use it. - Network Security: Treat cloud servers like you would internet-facing servers (because they are). Use cloud firewalls to restrict which IPs and ports can access your instances. If you have a web application, maybe only port 443 (HTTPS) is open to public, everything else is closed. Cloud providers often have security services (like AWS Security Groups, Azure NSGs) to easily set these rules. Also consider using a VPN or private connectivity for sensitive data transfer between your office and cloud (especially for hybrid clouds). Segment your cloud network – for example, databases might be on a private subnet with no direct internet access, only the application server can talk to them. - Logging and Monitoring: Turn on logging for cloud resources. Cloud providers offer tools like AWS CloudTrail or Azure Monitor that log every action (like who accessed what, or configuration changes). These logs are invaluable for audits or investigating incidents. Set up basic alerts for unusual activities – e.g., if someone tries to log in to the cloud console from an unrecognized location, or if a new server is spun up outside of normal patterns.

Many providers have free or low-cost security centers that will flag common issues (Azure Security Center, AWS Trusted Advisor) – check them regularly. - Regular Updates and Patching: If you're managing any servers (IaaS), ensure you update the operating system and software regularly. Cloud doesn't automatically mean your OS is updated (unless you use provider-managed services). Alternatively, use managed services where possible (for example, instead of running your own SQL server on a VM, use the cloud's Database as a Service – they handle patching). If using container images or virtual appliances from a marketplace, keep those updated too. - Backup and Disaster Recovery: Just because it's in the cloud doesn't mean it's backed up (unless you arranged it). Ensure critical data and configurations are backed up (many clouds let you take snapshots of servers or export data to storage). Ideally, store backups in a different region or an external system as well – that protects you if the cloud account is compromised or a region has an outage. And have a plan to restore (and test it). Some cloud services offer built-in redundancy – use them (e.g., geo-redundant storage). But also maintain your own copies for crucial data. - Secure Configurations: Always change default settings that could be insecure. For example, the default setting for some cloud storage might be no public access – good. But if you ever turn on public access for a folder, set an expiration or closely monitor it. Use provided security checklists: AWS has a "Well-Architected Framework" checklist, Azure has a Security Benchmark – they distill best practices. Implement basics like disabling SSH password login (use keys), rotating access keys regularly, and using service roles instead of embedding credentials in code.

The shared responsibility model also implies you should train your team on cloud security basics. Your developers or IT staff should know that, say, leaving credentials in code or mis-setting a permission could be disastrous even if the infrastructure itself is solid. Cloud providers often have free training modules on security – take advantage of those.

Case in point: a company had an incident where an old developer's cloud access wasn't removed – hackers breached that account. The provider's systems were not at fault, but the company hadn't managed IAM hygiene. With good role-based access and user offboarding processes, that risk could have been mitigated.

In summary, while cloud providers invest massively in security (and often can do a better job at infrastructure security than a small company could on its own), you cannot completely outsource security. You must lock your side of the house. The plus side is that most cloud platforms offer a wealth of security features – from identity management to network isolation – often more than what you had on-prem. Use them wisely.

Choosing the Right Cloud Approach

Not every cloud approach suits every need. Depending on your specific situation – type of data, existing investments, regulatory environment – you may choose public, private, or hybrid models (or a combination). Here's a simple guide:

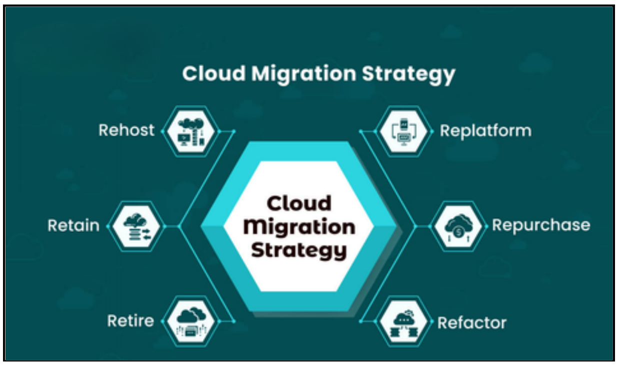
- **When is Public Cloud suitable?** For most businesses and most workloads, public cloud is a great fit, especially for new projects or digital services. If you have a standard web application, content website, mobile app backend, corporate email, collaboration software, etc., public cloud offers unbeatable scalability and cost-effectiveness. It's also ideal for dev/test environments because of easy spin-up/spin-down. Startups almost exclusively go public cloud to avoid CapEx. If your workloads don't involve ultra-sensitive data or extremely low-latency requirements tied to a physical location, there's a good chance public cloud will meet your needs. Today, even many banks and government departments use public cloud for non-core or even core workloads after proper risk assessments. Public cloud providers also offer virtual private clouds (isolated sections of the cloud just for you) which alleviate many multi-tenancy concerns.
- **When is Private Cloud better?** If you operate in a highly regulated industry or handle very sensitive data (think defense, certain government functions, perhaps some healthcare contexts), a private cloud might be mandated or preferable. Private cloud could mean using cloud software on your own servers (like running an OpenStack cluster in your office) or a dedicated portion of a provider's data center reserved for you. Large enterprises or govt agencies that require strict data sovereignty or have huge consistent workloads sometimes take this route.

Cost-wise, private clouds are usually viable for larger scale operations – an MSME generally wouldn't build its own private cloud due to high cost, unless it's via a community cloud offering (like certain state governments provide cloud infrastructure for local SMEs). A rule of thumb: if you have existing infrastructure and skills, and specific needs (legacy systems that won't run well on public cloud, for example), you might stick to private or on-prem for those while planning a slower transition.

- **When does Hybrid Cloud make sense?** Hybrid is often a transitional state or a deliberate strategy to balance requirements. If you have some systems that must remain on-prem or in a private cloud (perhaps due to latency – e.g., a factory control system that can't depend on internet connectivity – or regulatory issues), but you also want to leverage public cloud for other stuff, hybrid is the way. It allows you to connect your on-prem systems with cloud systems. Many organizations end up hybrid by necessity: for example, a company keeps large databases on-prem where they feel it's cheaper or safer (or due to data localization laws), but uses public cloud for running customer-facing web frontends and mobile apps that interface with those databases via secure links. Another use-case is disaster recovery: you run primary systems in your own small data center but use cloud as a backup environment in case of disaster (or vice versa). Hybrid setups can be complex because you have to manage two environments and ensure they talk securely (usually via VPN or dedicated circuits), but tools are improving to manage hybrid seamlessly (e.g., Azure Arc, AWS Outposts). It's best used if you truly cannot put everything on cloud (e.g., maybe an old ERP that runs on a proprietary hardware), or during a phased migration. A real example: many banks in India adopt hybrid – retaining core banking on their own IT, but using cloud for new analytics platforms or mobile banking front-ends to innovate faster while keeping core transaction data in-house.
- **Multi-Cloud considerations:** Multi-cloud means using more than one public cloud provider either for different applications or even splitting an app across them. The benefit is avoiding reliance on one vendor (mitigating lock-in) and potentially leveraging the best specific services of each. Some also do it for resilience (if one cloud has an outage, they can switch to another, though that's complex to achieve fully). However, multi-cloud introduces complexity – your team needs to learn multiple platforms, and your applications need to be cloud-agnostic which can limit using unique features. Multi-cloud makes sense if, say, you want to use Google Cloud's AI services for some workloads but Azure for your Microsoft-integrated systems, or if as a policy you don't want all eggs in one basket.
- For an MSME or single department, multi-cloud might be overkill unless executed via a managed platform that abstracts it. The key is to not inadvertently become multi-cloud without strategy – e.g., marketing team goes to one, finance to another, creating silos. If you do pursue multi-cloud, establish which workloads go where and ensure proper governance across them.

In summary, choosing the approach requires assessing what you need in terms of control, security, flexibility, and cost. Public cloud is like public transport or ride-share – efficient and flexible, but you share the highway. Private is like owning a car – more control, but higher responsibility and cost. Hybrid is maybe owning a car but also using public transport when convenient – requires coordination. There's no one-size-fits-all, and many organizations actually use a mix (e.g., email on public SaaS, highly sensitive database on-prem, etc.). For an MSME, jumping straight to a full private cloud is rare – usually the question is how much to put on public cloud vs what to keep in-house.

It's worth noting that the trend is towards more comfort with public cloud even for critical workloads as providers have addressed many security and compliance concerns. We also see niche community clouds – for example, certain countries have national clouds for government use, and sectors like banking have consortium clouds. The landscape is evolving, but the key is understanding your own risk appetite and requirements, then picking the model that fits.



Migration Strategy & Roadmap

Once you decide to embrace cloud, the actual migration needs a solid strategy. Rushing in without a plan can lead to cost overruns or technical snags. Here's a practical roadmap:

1. Discovery and Assessment: Take stock of all your current applications and data. What do you have running, on which servers, and what are their dependencies? Also classify data by sensitivity. This is like making an inventory before a move. For each system, note its performance needs (CPU, memory), storage size, usage patterns (24/7 vs periodic), and any compliance requirements. There are tools that can assist (cloud providers often have assessment tools or you can hire consultants for a cloud readiness assessment), but even a spreadsheet list maintained by IT can do.

For example, an MSME might list: ERP on local server (SQL database, used by 20 users, must be available 9-5), File server (~2TB files), Website on a shared hosting provider, 10 desktop PCs with certain software, etc.

2. Classify Workloads (The 6 Rs): Cloud migration pros often talk about the "6 Rs" for each application: Rehost, Refactor, Revise, Rebuild, Replace, Retain (different sources have slight variations).

3. Rehost (lift-and-shift): Move the application as-is to the cloud (e.g., take a VM image of your server and run it on a cloud VM). This is quickest but doesn't give cloud-optimized benefits.

4. Refactor (or Replatform): Make minor adjustments to use cloud services. For instance, move the app but use a cloud database service instead of running your own DB on a VM, so you don't manage that.

5. Revise or Rearchitect: Make more significant code changes to suit cloud (e.g., break a monolith into microservices, or adopt a cloud-native architecture). This is more effort but can pay off in scalability.

6. Rebuild: Scrap and rewrite from scratch on the cloud platform (for apps that are too inflexible to migrate otherwise).

7. Replace: Ditch the custom app entirely and use a SaaS alternative. For example, instead of migrating your legacy CRM, you might just adopt a new cloud CRM and export-import the data.

8. Retain: Keep it as is (on-prem) for now. Not everything must move; if something works well on existing setup and cost to move is high or risk is high, you can keep it (at least for now).

9. Retire: Decommission things that are no longer needed rather than moving them.

Go through each item from step 1 and assign one of these strategies. For example, you might decide to Rehost your ERP to a cloud VM since it's not easily changed, Refactor your customer portal to use a cloud database, Replace your on-prem email server with Office 365 (SaaS), Retain your factory's machine control system on-prem for latency, and Retire an old software that is no longer used.

1. Start with Non-Critical or Easy Wins: It's usually wise to first migrate something non-critical or easy to move, to get experience.

This could be moving your backup solution to the cloud, or your development/test environment, or an internal tool. The learnings here will help in bigger moves. It also builds confidence across the team. If possible, avoid making your very first cloud project a high-stakes one (like your core banking system or your primary database) – get some cloud "flight hours" on simpler systems first. An MSME might start by moving email and documents to Google Workspace or Office 365 (a fairly standard move with lots of community guidance) before tackling their ERP.

2. Plan Data Migration, Integration, and Testing: Moving large volumes of data can be one of the trickiest parts. Decide how you will transfer data – over the internet (might be slow for TBs) or via a physical transfer service (some clouds allow you to ship them a disk). Also plan how you'll keep data in sync during a transition period (maybe you have to run old and new in parallel for a bit). Integration: ensure your on-prem remaining systems can talk to the new cloud ones – usually via a secure VPN or direct connect. Testing is crucial: before decommissioning the old system, test the new cloud setup thoroughly. Does the application work end-to-end? Are all the users able to access it? Is performance acceptable? For example, if your accounting software moves to cloud, try generating reports, entering transactions, connecting any third-party tools, etc., to ensure all good. Have a roll-back plan: for each step of migration, plan how to revert if something goes wrong (maybe keep the old server running and untouched until the new environment is verified).

3. Set up Governance: cost, security, tagging: As you move to cloud, establish governance from the start.

4. Cost monitoring: Use the cloud's billing alerts or a third-party tool to track spending. Set up a simple process: e.g., the accountant or IT lead reviews the cloud bill monthly to catch anomalies. Tag resources by project or department to see who's spending what.

5. Security baseline: Align cloud security with your policies. That means enabling MFA on cloud console accounts, ensuring proper role-based access (not everyone should have admin rights to the whole cloud account), and applying any industry guidelines (e.g., if you're in healthcare, ensure the cloud setup meets required standards for data privacy – which often means encryption and access logging).

6. Configuration management: Decide on naming conventions and tagging for cloud resources to avoid sprawl (like name servers as "Dept-Function-Number" so it's clear, tag with environment like Production/Dev). Also decide who can provision new resources – you might not want every dev spinning up costly VMs without oversight.

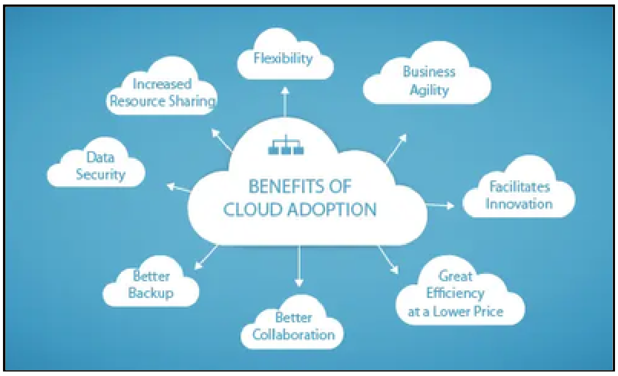
7. Backup and continuity in cloud: Ensure that whatever you move is also getting backed up (cloud is reliable but data deletion due to human error can happen anywhere).

Many people assume "cloud = automatically safe," but you often still have to configure backup or snapshots. Do that early.

8. Compliance in cloud: If you have to comply with something (ISO, GDPR, etc.), use the cloud's compliance resources. Major clouds provide compliance documentation and features to help (like Azure has blueprints for certain standards). Incorporate cloud assets into your audits/checklists.

9. Scale and Optimize Continuously: Cloud migration is not a one-time project – once you're in cloud, you should continuously optimize. The beauty of cloud is you can adjust on the fly: for example, after a month in cloud, you notice the server you migrated is only using 30% CPU; you can downgrade to a smaller instance to save cost. Or you find that a new cloud service could replace an older approach (like moving from a cloud VM running MySQL to a managed database service for easier maintenance). Set a cadence (maybe quarterly) to review: performance (are users happy? if not, scale up or use better architecture), cost (any resources idle or over-provisioned?), and new features (cloud providers add features – e.g., a new AI service might do something you were doing manually). Also, train continuously – ensure your team stays up to date with the cloud platform's updates (they have blogs, webinars – encourage your IT folks to spend a few hours monthly on this). This way, you fully leverage cloud over time, not just treat it as "another data center."

Throughout migration, communicate with stakeholders (users, management). Let them know what to expect – e.g., "This Friday we'll switch to the cloud system, there might be an hour of downtime." Post-migration, highlight wins ("reports are now generated in 5 minutes instead of 5 hours" or "we saved ₹50k this quarter after moving to cloud"). This builds momentum and buy-in for further cloud initiatives.



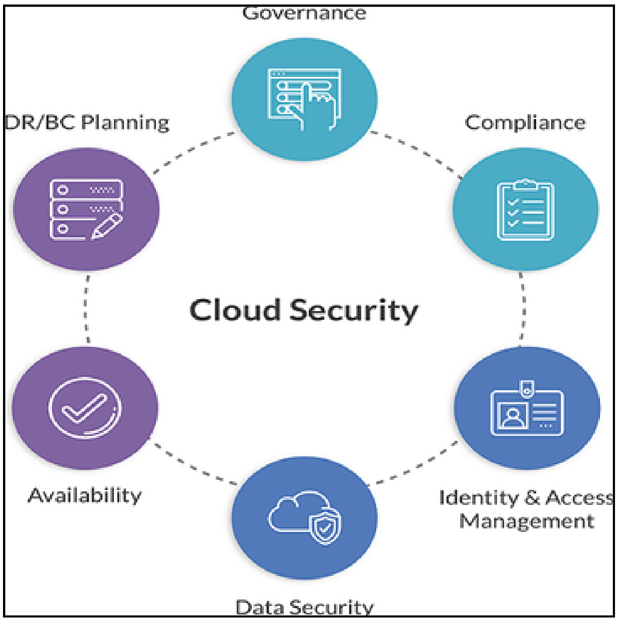
Risks and Challenges of Cloud Adoption

- **Security & Privacy:** Placing data on someone else's servers can feel risky, and breaches do occur (often due to misconfiguration). Pitfall: A small business left a storage bucket open and a lot of customer data was leaked. Avoidance: Understand your cloud's security settings or hire someone to set them correctly. Use encryption and strong access controls as described.
- Also, trust reputable providers (they invest heavily in security – e.g., RBI's Governor noted UPI and cloud have robust security for payments, with cloud handling ~80% of India's digital transactions). Still, don't upload sensitive data to cloud services without ensuring compliance. E.g., for personal data, perhaps choose a data center in India or use a provider certified for data protection. Keep local backups of critical data (in case of a cloud outage or account issue) – don't have a single point of failure.
- **Compliance & Data Localisation:** Pitfall: An Indian pharma SME used a US-based cloud to store trial data and later realized it violated an Indian regulation about keeping medical data within India. Avoidance: When dealing with regulated data, choose local regions or approved cloud providers. Many global clouds have Indian regions now – use them if required (e.g., an MSME working on a government project might be asked to use MeghRaj or an INDIACLOUD if specified). Keep documentation of where data resides and who has access, so you can demonstrate compliance if audited.
- **Vendor Lock-In:** Pitfall: A startup built heavily on proprietary AWS services (like DynamoDB, Lambda). When a big client mandated Azure for hosting, they struggled to migrate due to lock-in. Avoidance: If you worry about lock-in, design with portability in mind: e.g., use standard databases like PostgreSQL (which multiple clouds offer) instead of a cloud-specific one; containerize apps so they can run anywhere. Or use multi-cloud management tools or abstracts (though these add complexity). Some vendor lock-in is almost inevitable (each cloud has unique aspects), but you can mitigate by not using too many niche services unless necessary, and by keeping backups of data in standard formats regularly – so if you had to switch cloud, you have your data.
- **Cost Overruns & Shadow IT:** Pitfall: After moving, an MSME's cloud bill kept climbing; various team members had launched test servers and forgotten them. The finance head was shocked at the quarterly invoice. Avoidance: Implement cost controls – set budgets, get notified when spending hits 80% of budget. Use tag-based cost reports to identify cost centers. Institute an internal policy: e.g., "Any new cloud resource over ₹X per month cost needs approval" or "Dev servers must be turned off at night/weekends." Also educate teams that cloud isn't free – you pay for what you use, so they become mindful (like turning off lights when leaving a room). Use automation: many clouds let you schedule stop/start of instances (so dev VMs turn off outside work hours to save money). Address shadow IT by having an IT steering small committee that evaluates new SaaS subscriptions, so they can consolidate if multiple teams seek similar tools.

- **Skill Gaps & Misconfigurations:** Pitfall: A company moved their website to cloud but misconfigured the DNS and it was intermittently down for weeks – they just lacked the skill to set it up right. Avoidance: Invest in training your IT person (cloud providers have free tiers and training modules). Or use a managed service provider to do the migration and maybe ongoing management until your team is comfortable. Many SMBs use local IT firms or cloud consulting partners for the initial setup. It's worth the one-time cost to avoid costly mistakes or downtime. Over time, internal staff can learn by shadowing these experts. Additionally, consider starting with higher-level services (SaaS) which require less skill – e.g., instead of putting up your own server for an e-commerce site, maybe use Shopify or Azure's fully managed web app service.

To sum up, cloud adoption comes with new responsibilities. The cloud providers give you powerful tools – but you have to use them correctly. With planning and sound management, the challenges are manageable. Many MSMEs already navigated this successfully: a NASSCOM survey indicated that by 2025, over 60% of small businesses in India were expected to have some cloud footprint, navigating compliance and security via proper guidance.

Think of moving to cloud like moving to a sophisticated office building – the infrastructure (elevators, security, utilities) is world-class, but you still need to lock your office door and decide who gets keys, and you need to pay the rent on time. Do those, and you can enjoy the high-tech environment without issues.



Cloud Security Essentials – Shared Responsibility (Recap)

Since security is such a big concern, it's worth briefly recapping the shared responsibility model and key tips (because it cannot be stressed enough): - Cloud provider secures the cloud itself (data center, physical security, foundational services).

You secure what you put in the cloud (OS, applications, customer data, user permissions). - Enable MFA on all cloud admin accounts – most cloud breaches of SMEs happen because of stolen passwords without MFA. - Never expose more than necessary: If an application doesn't need to be public, put it on a private network. If it must be public, lock down ports and use security groups. Use VPNs or remote desktops to access cloud VMs rather than opening management ports to the internet. - Encrypt your data at rest: All major clouds let you encrypt storage and databases with a click – do it, especially for sensitive info. Similarly, enforce TLS (HTTPS) for data in transit. - Backup data in cloud: Ideally, setup backups that go to a different region or even download key backups to on-prem occasionally. And consider enabling cloud features like versioning (for storage) to recover from accidental deletions or ransomware (yes, ransomware can hit cloud drives too if synced). - Least Privilege Access: Make sure each user in your cloud account has only the permissions needed. E.g., developers can manage dev resources but not touch production databases; a vendor who manages one application gets access only to that app's resource group, not the entire account. - Monitor and Audit: Turn on cloud logging and periodically review or set alerts. Many SMEs integrate basic alerts to an email or a messaging app – e.g., "alert if any resource is made public" or "alert if unusually high network traffic." Some cloud platforms offer free security scorecards – review them and fix the high-risk items they flag.

By following these practices, even a small business can achieve a security posture in the cloud on par with much larger companies. Don't be intimidated – leverage provider documentation and maybe community forums if unsure how to do any of the above; there's a lot of guidance out there.

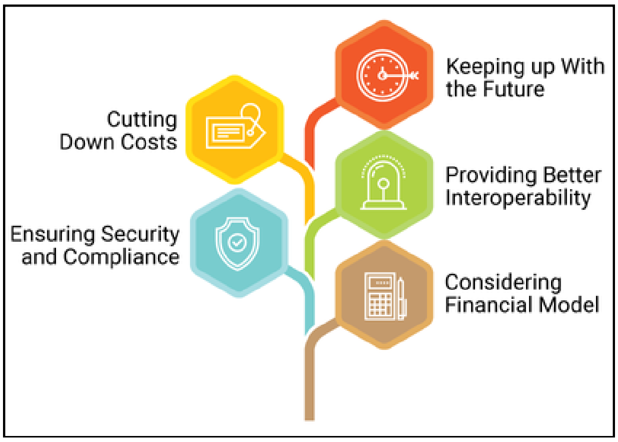
Migration Strategy & Roadmap (Recap for Cloud)

(We discussed a roadmap earlier in the AI section; here's a cloud-specific abbreviated roadmap as a takeaway.)

1. Plan and Assess: List your apps and decide which to move (e.g., email and website first, core ERP later). Evaluate technical needs and choose the right cloud model for each (public/private/hybrid).

2. Pilot on Cloud: Start with a non-critical service on the cloud to get familiar. For example, move file backups or a small internal tool first.

3. Migrate Step-by-Step: For each system, choose migration approach (lift-and-shift vs. replace with SaaS, etc.). Execute during a low-business period if downtime needed. Use available migration tools (many cloud vendors have free migration utilities or programs for SMEs).



4. Verify and Optimize: After moving a system, test thoroughly and optimize its cloud resources (rightsizing VM types, etc.). Address any performance or cost surprises.

5. Train Team and Adjust Processes: Ensure your team knows how to operate in the new cloud environment (e.g., how to deploy new code to the cloud server, or how to retrieve logs now). Update documentation and responsibilities accordingly.

6. Secure and Govern: Immediately implement security basics (as covered) for the new cloud setup and set up budgets/alerts for cost control. Don't postpone these – it's much easier to build good habits from day one than to rectify lax practices later.

By following this, you'll avoid the common missteps that give cloud projects trouble (like migrating too much at once, or leaving security holes in the rush to go live).

Governance, Finance and Procurement View

Adopting cloud has implications beyond IT – it affects finance, procurement, and corporate governance:

- **Role of CFO and Finance Team:** In the on-prem world, IT costs were largely CapEx (buying assets) with depreciation. Cloud turns many of these into OpEx (monthly operational expenses). The CFO will want to manage this shift – OpEx adds flexibility but also requires vigilant monitoring to avoid ballooning costs. Finance should establish processes to review cloud spend. For instance, set a policy that IT must provide a quarterly cloud spending report with explanation for variances. Use tagging to align costs with departments or projects, so the finance team can see ROI per project. Also, with cloud's elastic nature, finance might involve in decisions like whether to commit to reserved instances (pay upfront for lower running cost) or stay completely pay-as-you-go. The CFO should also ensure any cloud contracts meet company policies – e.g., data ownership clauses or exit clauses are reviewed (so you don't get stuck or face hidden charges).

- **Internal Audit and Risk:** From a governance perspective, internal auditors will need to update their controls for a cloud-centric environment. This includes checking: Do we have proper access controls on the cloud platform? Are we following data protection rules when using cloud services (who approved which data to go to cloud)? Is there a contingency plan if cloud services fail? They should audit things like whether cloud configuration best practices are followed (there are automated tools that can generate compliance reports for cloud setups – the IT team can run these and provide to audit). Auditors will also consider vendor risk – what if the cloud provider faces an outage or breach – do we have mitigating arrangements? It might sound like overkill for a small firm, but even a simple yearly checklist (like: verify backups in cloud work, verify only authorized personnel can spin up servers, etc.) is worth doing internally.

- **Procurement and Vendor Management:** If switching to cloud, you might be dealing with fewer hardware purchases but more service procurements. Procurement should ensure cloud contracts have clear SLAs (Service Level Agreements) – what uptime is guaranteed, what compensation if any for outages, etc. Pay attention to exit clauses – can you get your data out easily if you switch providers, how long will the provider retain your data (you don't want them deleting everything the moment you stop service, or conversely holding it hostage). Data ownership should be clearly yours as per the contract. Also, procurement might need to adapt to continuous spend – instead of one-time asset buys, cloud is a continuous service, sometimes requiring different approval workflows (maybe a larger delegation for monthly cloud bills vs. capital spends).

- **Vendor Lock-in Mitigation**: As part of governance, management might set a strategy to avoid excessive lock-in. This could include multi-vendor strategy for critical applications or negotiating contracts that allow portability (for example, ensuring you can download your entire data in a standard format periodically). It's a balance – chasing multi-cloud can diminish efficiency, but being too locked can be risky.

- Governance bodies (or simply the owner and tech lead in a small company) should periodically review if they're comfortable with the dependency profile.
- **Regular Cost and Performance Review:** Cloud models introduce the need for ongoing oversight. It might be wise to have a monthly meeting (even 15 minutes) between finance and IT to go over cloud usage and costs. This keeps surprises away and allows course correction (e.g., "this app is costing too much, let's refactor it this month to a cheaper model"). It also helps finance understand IT needs ("we're spending more because traffic grew 50% – which is a good thing, but maybe we commit to a reserved plan to save costs").
- **CFO and Internal Audit Involvement in Cloud Strategy:** Getting buy-in from finance early can smooth cloud adoption. For example, the CFO's perspective might highlight the need for chargeback mechanisms – making departments aware of their cloud usage costs. Internal audit's early involvement ensures compliance issues are flagged while plans can still be adjusted (e.g., audit might say, "if we move payroll data to cloud, we need to ensure it's within India" – knowing that upfront is crucial).

In essence, treat cloud not just as an IT project but as a business transformation. This means involving cross-functional leadership in decisions. Many large firms have Cloud Councils or similar – at an MSME, it could just mean the owner, IT lead, and finance head have a joint say in major cloud-related decisions, balancing innovation with oversight.

Future Trends Leaders Should Watch

The cloud landscape evolves rapidly. Leaders should keep an eye on trends that could impact how they use cloud in the next 3–5 years:

- **Serverless and Function-as-a-Service:** We touched on this – serverless computing (like AWS Lambda, Azure Functions) lets you run code without managing servers at all. It's event-driven (code runs only when triggered) and highly scalable automatically. This can further reduce cost and ops overhead for certain tasks. Many foresee a future where lots of backend logic for SMEs could shift to serverless for simplicity. As these technologies mature, consider where you might replace a constantly-running server with a serverless function.

- For instance, an MSME that currently runs a small server 24/7 to process a few daily tasks might save by shifting that to serverless, paying only per execution. Leaders should watch cost models and tooling improvements in this area.

- **Edge Computing and 5G:** As 5G networks roll out, the idea of edge computing – processing data closer to where it's generated – is gaining traction. Cloud providers are extending services to the edge (e.g., AWS has "Outposts" and Azure "Edge Zones" that bring cloud capabilities on-prem or to cell towers). For industries like manufacturing or retail, this could mean ultra-low latency analytics on site, with aggregation to cloud. Imagine a factory where AI quality inspection happens on an edge device in real time (no round trip to a distant cloud), but summary data and heavy model training still happen in cloud. Or a retail chain where each store has a mini-cloud node for quick response (say for checkout systems), synced with main cloud. If your business could benefit from <10ms latencies or has huge data that's expensive to constantly upload, edge might become relevant. However, it's a bit early for many SME use cases – but keep an eye as providers are making it more accessible.
- **Industry-Specific Cloud Solutions:** Big cloud players are creating tailored solutions – e.g., Banking Cloud, Healthcare Cloud – which come pre-configured for certain compliance and have industry-specific tools. In India, we see initiatives like a Cloud for Government or SME-focused cloud marketplaces. Over the coming years, leaders should watch if their industry gets such specialized offerings because they might simplify adoption (for example, a healthcare cloud that is automatically HIPAA compliant could save a lot of setup effort).
- **AI and Cloud Convergence:** We are already witnessing how cloud is the backbone for AI. The latest generative AI models (like ChatGPT) are delivered via cloud APIs. AI-as-a-service will proliferate – meaning even smaller firms can utilize advanced AI without building infrastructure.

- For instance, you might not need your own data science team to benefit from AI – you can call a cloud AI service to translate, summarize, predict, etc. as needed. Leaders should consider how "AI at your fingertips" via cloud could open up new business processes or offerings. On the flip side, running your own AI models (if you have proprietary data and need custom models) is becoming easier with cloud GPU offerings. The trend is that cloud providers are embedding AI into many services (e.g., database services with AI that auto-tunes queries, or AI that monitors security logs). So using cloud not only gives raw compute, but built-in intelligence. Stay updated on these features as they might quietly improve efficiency if turned on.
- **Sustainability Requirements:** There's growing emphasis on greener IT. Interestingly, using cloud can be more energy-efficient than many small on-prem servers because cloud data centers optimize resource use and power. Some large clients and regulators will start asking for carbon footprints of IT operations. Cloud providers are moving toward renewable energy and offer carbon footprint tools. An MSME might soon be asked by a client, "Are you using sustainable practices for your IT?" – being on a major cloud that is powered 100% by renewable energy (as some aim to be by 2030) could become a selling point. Leaders should follow sustainability reports of their cloud vendors. Also, concept of FinOps (Financial Operations) came to manage cost, now GreenOps might become a thing – managing cloud usage for minimal environmental impact (e.g., scheduling non-urgent batch jobs to times when data centers have excess renewable power).
- **Regulatory and National Cloud Policies:** In India, we might see more directives or incentives around cloud adoption, data sovereignty, etc. For example, government tenders might start stipulating use of MEITY-approved clouds, or data localization might tighten requiring in-country clouds for certain sectors. Leaders should watch announcements from bodies like MEITY, RBI, etc. about cloud guidelines. Engaging in public-private forums (like NASSCOM SME events on cloud) can give heads-up on where policy is headed (e.g., more support for MSME cloud training, or stricter cybersecurity mandates).
- **Multi-Cloud and Cloud Brokerage:** Tools to seamlessly use multiple clouds or switch between them are getting better (though still evolving). If these mature, vendor lock-in fears might reduce. We might see a rise of cloud broker services – where an SME can just state needs and a broker finds best fit across providers dynamically (somewhat like how you buy bandwidth from an ISP without caring which fiber they route through). While it may not directly affect an MSME manager's daily decisions yet, it could in future mean more flexibility and perhaps better pricing competition among clouds.

The pace of innovation is such that leaders don't need to implement everything cutting-edge, but they should stay informed and be ready to pilot new ideas when there's a clear benefit. Cloud providers often preview upcoming tech – following their blogs or joining user groups can give you inspiration on what's possible.

In essence, cloud is not a static destination but a continuously advancing toolbox. A forward-looking leader treats it as a strategic asset – not just an IT outsourcing. That means periodically revisiting your cloud strategy to incorporate new capabilities and ensure it aligns with business goals (e.g., if quick customer service is a differentiator, explore the latest cloud AI chatbot; if cost leadership is key, adopt the newest cost-saving cloud feature).

Conclusion: A Balanced, Thoughtful Cloud Journey

Migrating to the cloud is not an "all or nothing" decision, nor is it a one-time event. It's a journey – one that should be aligned with your business strategy and risk profile. We've seen how cloud computing can offer substantial benefits: cost flexibility (turning large capital outlays into manageable pay-as-you-go bills), agility (spinning up resources in minutes, enabling faster innovation), resilience (geographically distributed systems reducing downtime), and collaboration (anywhere access empowering remote work and cross-location teams). These translate into very real business outcomes: faster time-to-market for new projects, easier scalability when your business grows or enters new regions, and often improved service reliability for your customers or users.

However, we've also discussed the risks and responsibilities that come with cloud adoption. Security and compliance remain paramount – moving to the cloud doesn't eliminate them, it changes their form. Cost management requires new discipline to avoid surprises. Vendor dependence must be consciously managed. And your people need to be brought along through training and clear governance.

For decision-makers in PSUs, MNCs, government departments, or MSMEs, the key is to approach cloud migration in a balanced and thoughtful way: - Strategic Alignment: Why are we moving to the cloud? Be clear on objectives (cost saving, modernizing an old system, enabling remote access, etc.). Move systems that further those objectives and hold back where cloud may not add value. - Gradual Adoption: You need not bet the farm on day one. Start with a pilot or a non-critical function (as we outlined) – get a quick win, then iterate. This reduces risk and builds confidence. Many successful cloud journeys began with moving email and a couple of apps, and over 2-3 years ended up mostly in cloud after gaining trust in it. - Invest in People: Ensure your IT team (or whoever manages your systems) is trained or supported through the transition. Encourage a culture of continuous improvement – cloud offers so many features that you'll keep discovering optimizations over time. - Monitor and Adapt: Cloud isn't set-and-forget. Use the analytics and monitoring available to keep an eye on performance, security, and spend. The beauty is you often have more visibility than on-prem (dashboards, logs, AI insights). Set up a cadence in management reviews to consider these reports, so cloud usage stays optimal and aligned with business needs. - Don't Forget Plan B: Hope for the best, plan for the worst. Even as you enjoy cloud benefits, have contingency plans (e.g., if your cloud provider has a major outage, do you have a way to operate for a day? Maybe having critical files also synced to a local device, or an alternate way to communicate with customers). Cloud failures are rare but not impossible – being prepared keeps you resilient.

Above all, view cloud as a strategic decision, not just an IT upgrade. It can transform how you operate – enabling new business models (for instance, offering your software product on the cloud as a service rather than on CDs), improving customer experiences (through better uptime and responsiveness), and even impacting valuations (investors often value companies with scalable cloud-based infrastructure higher than those with heavy legacy baggage). But to reap these rewards, leadership involvement is essential – it's not something to delegate entirely to IT. Successful cloud adoption in organizations large and small has top management championing it, addressing the change management (both technical and human).

In conclusion, cloud computing has proven it's not a passing trend but a foundational element of modern business infrastructure. The question for most organizations is no longer "Should we use cloud?" – it's "How much, how fast, and in what ways should we use cloud?". By taking a measured, well-governed approach, you can significantly tilt the balance towards the benefits while mitigating the risks.

So consider this a call to action: identify a small pilot (be it migrating an application or adopting a new SaaS tool) and give cloud a try in an area of your business that could use a boost. Learn from that, then expand. With each step, you'll build confidence and capability. Many of your peers are already on this journey – India's cloud market is booming with over 90% of organizations using cloud in some capacity, and government and private sector initiatives are accelerating digital transformation. Don't be left behind on the ground; elevate your operations to the cloud, one thoughtful step at a time. The sky (or should we say the cloud) is not the limit – it's the new beginning.

CMA Rohan Sharma

CMA Rohan Sharma is a finance professional and mentor known for helping CMA students and fresh graduates build strong careers. With experience in costing, taxation, budgeting, and SAP FICO, he has guided thousands through his platform Career Success Launchpad. His simple teaching style and practical insights have helped many learners secure roles in PSUs, MNCs, and top corporates. He is SAP FI & CO Certified with 7 years of corporate experience.

FCMA, Interview Coach
Editorial Board Member, The Worldonomics Times

Cybersecurity Basics: Essential Steps for Protecting Small Business Data from Common Threats

Introduction

Cybersecurity as a Business Survival Issue

Late one night, the owner of a small vendor company receives a chilling message on her computer screen: "Your files have been encrypted. Pay ₹5 lakh in Bitcoin or lose everything." Just hours before an important tender deadline, ransomware had locked her out of all documents. This nightmare scenario is far from rare. In recent years, cybercriminals have increasingly targeted small and medium businesses, knowing that these organizations often have weaker defenses but valuable data. Studies show that around 46% of all cyber breaches impact businesses with fewer than 1,000 employees, and 61% of SMBs (small and mid-size businesses) reported being the target of a cyberattack in a single year. The consequences can be devastating – the average cost of a small business data breach is about $120,000 (roughly ₹1 crore) when you factor in downtime, lost sales, and recovery expenses. It's no surprise that an estimated 60% of small companies that suffer a major cyber attack end up closing their doors within 6 months.

Clearly, cybersecurity is not just an "IT problem" – it is a core business survival issue. It's about protecting the money in your bank, the trust of your customers, and the proprietary information that keeps you competitive. Importantly, cybersecurity is as much about people and processes as it is about technology. Various analyses have found that anywhere from 68% to 95% of breaches involve some form of human error or negligence. In other words, even a state-of-the-art firewall won't help if an employee is tricked into giving away the keys to the safe. That's why building a security-conscious culture and following basic best practices can dramatically improve your defenses, even on a tight budget.

In this article, we'll break down common threats in plain English and outline essential steps – mostly simple and low-cost – to protect your small business data.

Think of it as a practical cybersecurity playbook for MSMEs, startups, and any organization where dedicated security teams might be lacking. Whether you're a manufacturing unit supplying a PSU, a retailer handling customer credit details, or a government office digitizing its records, the principles remain the same. Let's dive into the threats you face and, more importantly, how to counter them.

Common Threats – Explained in Plain English

Cyber threats might sound abstract or overly technical, but at their core they often exploit very human flaws. Here are some of the most common threats to small businesses, explained with simple scenarios:

- **Phishing and Social Engineering:** Imagine you get an email that looks like it's from your bank, asking you to verify your account due to "urgent security issues." It has your bank's logo and a convincing tone. If you click the link and enter your password on the fake site, you've just handed it to a scammer. That's phishing – fraudulent emails or messages designed to trick you into revealing sensitive info or installing malware. Social engineering extends beyond email: a fraudster might call pretending to be a client or IT support to extract information ("I'm from your software vendor, we need your login to apply an update"). They might send a WhatsApp message with a link to "claim a prize" that actually steals your data. Essentially, these attacks prey on trust and human nature – they con you into bypassing security yourself.

Real-world example: A Pune-based MSME's accounts officer got an email that appeared to be from the CEO, urgently requesting ₹2 lakh to be transferred to a new vendor account for an "emergency shipment." Thinking it was genuine, she made the transfer – only to find out later the CEO never sent such an email. It was a business email compromise scam. The email address was spoofed to look like the CEO's, and because the request was urgent and from "the boss," normal checks were skipped. Phishing can also target your customers – e.g., spoofing your company's email to send fake invoices. The key point: if it's digital and requesting something sensitive or valuable, be suspicious. Always verify through a second channel (a phone call to the supposed sender, for instance).

- **Malware and Ransomware:** Malware is malicious software – viruses, worms, trojans – that can infect computers and cause damage. They often arrive via email attachments ("invoice.zip"), downloads from untrusted websites, or infected USB drives. Once malware is in, it can do things like steal data, give hackers remote control, or encrypt files.

Ransomware is a type of malware that locks your files and demands payment for the key (as in our opening story). It has hit countless small businesses, from local retailers to small clinics, often via an employee clicking a bad link or opening an attachment.

Scenario: A small design agency found that one employee's computer had a pirated software installer which quietly installed a keylogger (spyware). Over weeks, it captured passwords to the agency's email and cloud storage. The hackers used those credentials to steal client project files and then attempted to extort the agency, threatening to leak the designs unless paid. This happened not because of some high-tech hack, but because of an unguarded install of pirated software that contained malware. Ransomware cases similarly often start with one wrong click. The results can be devastating – imagine all your billing records, GST filings, and customer orders suddenly inaccessible. Statistics suggest an attack on a business occurs every 11 seconds on average globally (many are ransomware), and 51% of businesses hit by ransomware end up paying the ransom (often because they lacked backups). The best defenses here are prevention (good antivirus, cautious behavior) and preparation (have backups so you don't have to pay ransom).

- **Credential Theft and Password Reuse:** Many breaches occur without any fancy malware – hackers simply log in using valid credentials (username & password) that they obtained. How do they get these? One way is phishing (they trick someone into entering credentials on a fake site). Another is through data breaches on other services – for example, a small business owner uses the same password for their personal Gmail as for the company VPN. If Gmail or some other site gets breached and that password leaks online, attackers will try it on the company VPN (this is called credential stuffing). Unfortunately, password reuse is very common. One study found 91% of users reuse passwords across sites, and 80% of hacking-related breaches involve stolen or weak passwords.

Example: A sales manager at an MSME uses the same password for a job search website and the company's order management system. The job site gets hacked, the password becomes public. Cybercriminals, using automated tools, try that email and password on various business systems – they get into the order system and download the customer list and pricing data. Next thing the MSME knows, a competitor somehow has their client list (because the hackers sold it). All because of one reused password. The lesson: use strong, unique passwords and enable two-factor authentication. A password manager tool can help create and remember unique logins for each service. It's a bit of upfront effort but saves huge pain later. If remembering dozens of passwords is hard (it is), a simple practice is at least to never reuse your work passwords on any personal or third-party site.

- **Insider Risks (Careless or Malicious Staff):** Not all threats come from outside. Employees or trusted partners can accidentally or intentionally cause breaches. Careless insiders might click on phishing emails, use weak passwords, lose a laptop, or send the wrong attachment to a client. Malicious insiders could steal data (an employee leaving to start a competing business copying the customer database), or sabotage systems (rare but it happens, e.g., a disgruntled IT admin wiping data). According to some reports, about 35% of data breaches involve internal actors – often due to mistakes rather than malice, but both count.

Scenario: A well-meaning HR assistant at a small firm receives a call that appears to be from the company's IT service provider, asking for her system password to "apply urgent security updates." She provides it (they sounded convincing). In reality, it was a social engineering call. The attackers used her access to view HR files and got hold of employees' personal and bank details. This wasn't hacking in the Hollywood sense – it was exploiting the human trust factor. On the malicious side, consider a salesperson who knows she's being let go, so she downloads the entire client list to take to her next job. These insider incidents can be hard to prevent entirely. The key is creating an environment where employees know the rules (e.g., never give out passwords, follow data handling policies) and aren't given excessive access to things they don't need (principle of least privilege). Also, having audit logs – so if something fishy happens, you can trace it. For accidental risks, continual training (as we'll cover) is the antidote.

- **Third-Party and Supply Chain Risks:** Your business might be secure, but what about your vendors, suppliers, or service providers? Attackers often aim for smaller firms that are connected to bigger targets – this is called supply chain hacking. For example, your MSME could be a supplier to a large PSU. Hackers might try to breach you not for your data, but as a stepping stone to the PSU's network (maybe you have access to a procurement portal). Or consider software supply chains: if you use a certain software and that software's updates get compromised (like the infamous SolarWinds breach), it can affect you. · Additionally, you might rely on a third-party for IT support – if their systems or practices are weak, that's an indirect risk to you.

Example: A small logistics company used a third-party billing software. Hackers breached that software vendor and inserted a backdoor in a routine update. Through that, they accessed several of the vendor's clients, including the logistics company, stealing financial records. In another case, an SME that had a GeM (Government e-Marketplace) account got hacked via a weak password; the attackers then tried to use that to issue fake orders. So, connecting points can be abused. Mitigation includes due diligence on vendors (ask them about their cybersecurity), contractual requirements for security standards, and monitoring of third-party access. It's also a reason to not be complacent if you're part of someone else's supply chain – big clients now often require their vendors (even small ones) to follow cybersecurity best practices and might drop those who don't. This trend is growing – for instance, a McKinsey report noted e-commerce and digital trade growth also raises supply chain cyber risks, and it's pushing more security demands onto SMEs.

In summary, the threats range from high-tech (malware) to low-tech (con calls) – but all exploit weaknesses in technology or human behavior. The encouraging news is that by addressing some basic issues (strong passwords, up-to-date systems, user awareness), you can thwart the majority of common attacks. It's like locking your doors and windows – most thieves will move on to an easier target. In the sections below, we'll cover exactly those "lock the door" measures.

What Data and Systems Need Protection

You might think, "I'm a small business, why would anyone target my data? It's not like I have state secrets." But even ordinary business data can be gold for criminals, and some is critical for your operation. Let's identify what needs protecting:

- **Financial Records and Banking Info:** Your financial books (ledgers, accounting software data, tax filings) contain account numbers, transaction details, maybe even customer/supplier bank details. If criminals get those, they can commit fraud (like crafting very convincing fake invoices or phishing your clients). Or imagine losing all your financial data to a ransomware with no backup – how would you invoice or file GST? Also, your internet banking credentials – if those are stolen via keylogger or phishing, your bank account could be drained. One stat showed nearly 40% of small businesses have lost crucial data as a result of an attack, which often includes financial data. Protect this by securing accounting systems, using MFA for bank logins, and keeping backups of financial files.
- **Customer and Employee Personal Data (PII):** This includes things like customers' phone numbers, addresses, purchase history, as well as employee records (PAN, Aadhaar, salary details, health info). In wrong hands, these enable identity theft or social scams. Also, losing customer data will damage trust and could bring legal trouble under emerging data protection laws. For example, if you're an HR services firm storing candidate KYC documents, that's sensitive data that hackers would love to sell. A breach of employee data can also lead to financial frauds (imagine someone using leaked salary slips and PAN copies to take a loan in your employee's name – it happens!). So, identify where this data is stored (HR folders, CRM software, etc.) and ensure it has restricted access and encryption if possible.
- **Client Projects and Intellectual Property:** If you design products or write code or have proprietary formulas, that intellectual property is valuable. Even your quotation and costing data is sensitive – if a competitor steals your bid details, they can undercut you. There have been cases in India of hackers stealing tender bid files from one company to give to another for a fee. Or think of a small R&D company – their designs could be sold to a foreign buyer. Don't assume "we're small, no one wants our designs" – criminals might not know how big you are; they target broadly and see what they get. Any data that gives you a competitive edge or is core to your business (product designs, source code, proprietary process docs) should be well-guarded.
- **Operational Systems:** These include your email accounts, websites, databases, and any specialized software (CAD tools, ERP system, etc.). If email is compromised, it can be used to impersonate you (leading to phishing of your clients or instructions to your staff that are fake). If your website is hacked, it can damage your reputation (imagine your site defaced with a hacker message or containing malware that infects visitors). If an attacker gets into your database, they might alter or destroy data (for sabotage or ransom). Even machines in a factory that are controlled by computers could be targeted (though rarer, but not impossible – we've seen incidents of industrial control breaches in larger firms). Essentially, any system that, if disrupted, would halt your business or allow unauthorized actions, needs security. For example, a modest distributor might rely heavily on an online inventory tool – if an attacker locks it up or deletes records, trading halts.

- **Devices and Endpoints:** Laptops, smartphones, external drives – these physical devices often carry a lot of data. An unattended, unlocked laptop can be a thief's easiest hack (no need to bypass firewalls if the data's open on the screen!). The same with a lost company phone that wasn't set with a passcode – it might have your email auto-logged in and files in cloud apps accessible, essentially handing keys to an attacker. Endpoint security – ensuring devices have proper access control (passwords, PINs), and encryption – is vital. Many MSMEs allow staff to use personal devices for work (BYOD); that can be okay, but it means work data might live on a device that also has kids playing games on it and no antivirus. Make sure to at least encourage or mandate basic protections on any device that touches work data (like requiring a phone lock, ability to wipe it if lost, etc.).

In short, protect the data that could hurt you or others if exposed, and the systems that run your business. A quick way to prioritize: ask, "If this information leaked publicly, or this system went down for a week, how bad would it be?" If the answer is "quite bad," then secure it strongly.

It's also worth noting that if you handle data for bigger organizations (e.g., you're a vendor processing some data for a PSU or MNC), you likely have contractual obligations to protect it. PSUs have started auditing vendors' cybersecurity in some cases. So safeguarding that isn't just about you, it's about keeping contracts.

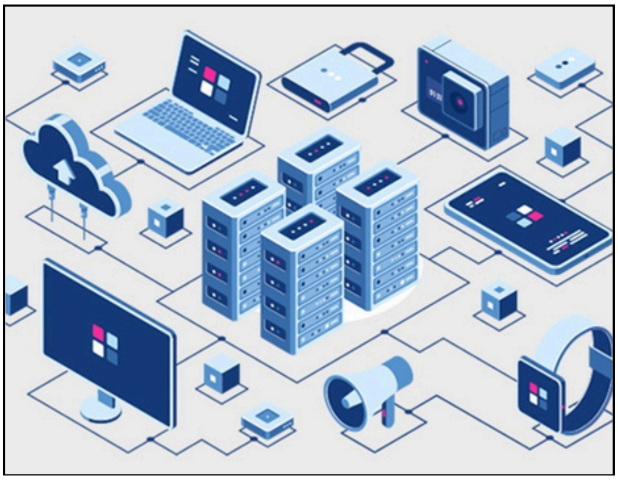
We'll now move on to how to actually secure these assets – starting with everyday practices (cyber hygiene) that drastically reduce risk.

Foundational Cyber Hygiene – The Essentials

Think of cyber hygiene as the digital equivalent of locking your doors, washing your hands, and not leaving valuables in plain view. These basic measures dramatically lower the chance of common cyber incidents and are within reach of even the smallest business. Let's outline an essential "to-do" list:

- **Identity & Access:** Use strong, unique passwords for all accounts – especially email, banking, servers, and admin accounts. A strong password means at least 12 characters, mix of letters (caps and lowercase), numbers, and symbols (or use a passphrase like "CorrectHorseBatteryStaple" which is long and easy to recall). Crucially, never reuse passwords across different services. If that sounds hard, use a password manager (there are good ones like LastPass, Bitwarden, etc. – some are free or low-cost for small teams). This way you only remember one master password and the tool handles the rest. This addresses the huge issue of credential theft; even if one password leaks, it won't open all doors. Next, enable multi-factor authentication (MFA) wherever possible – email, cloud apps, VPN, even social media.
- MFA typically means besides password, you need a code from your phone or a hardware token. It blocks over 99% of automated attacks cold. Many services offer SMS OTPs or authenticator apps – take those options. Also, avoid sharing accounts. Every user should have their own login where feasible, so activity can be traced and access revoked individually if needed. Limit admin privileges to those who truly need it and use separate admin accounts for high-level tasks (don't do daily work while logged in as system administrator). This way, if a regular user is compromised, the damage is limited.

On a practical note, implement a policy that passwords should not be simple or reused – encourage phrases or a mix. And maybe do a company-wide password reset periodically, especially if there's news of a breach involving an employee's email elsewhere (there are services and websites like "Have I Been Pwned" that let you check if emails appear in known breaches – useful for proactive resets).



- **Devices & Network:** Keep all software updated. Most malware and attacks exploit known vulnerabilities – the vendors already issued patches for them. Set Windows, macOS, Linux servers, and software like browsers to auto-update. Don't postpone those update reboots indefinitely. The difference can be huge: e.g., the WannaCry ransomware spread in 2017 largely hit systems that hadn't applied a patch available months prior. Similarly, update your phone OS and apps – mobile malware is less common but not unheard of. Install a reputable antivirus/anti-malware program on all PCs and ensure it updates signatures daily. Modern AV can catch many threats and some even have behavior monitoring to catch ransomware early. Windows 10/11's built-in Defender is actually pretty good if kept updated – many small businesses can use it if they can't invest in third-party solutions. Just make sure it's not turned off. For network, secure your Wi-Fi: change the default router admin password (attackers know default creds like "admin/admin"), use WPA2 or WPA3 encryption with a strong Wi-Fi key (no "12345678" or "company123" – make it complex).

- If you offer guest Wi-Fi, isolate it from your internal network so guests (or someone sitting in the parking lot) can't snoop your shared files or devices. If employees work remotely, encourage use of a VPN when on public Wi-Fi or provide a company VPN for accessing internal resources – this encrypts their traffic so even if they connect at a cafe, it's protected.

Another tip: turn off unnecessary services and close ports on your network and devices. For instance, if you don't use Remote Desktop, disable that port; if an IoT device has an open interface you don't use, shut it. And definitely change defaults on things like IP cameras or NAS boxes – default passwords on those are a known weakness. Ensure firewalls are enabled on PCs and any servers – the built-in OS firewalls are usually sufficient to block unsolicited inbound connections.

- **Email & Web Safety:** Think before you click – make this a mantra in your team. Train everyone to recognize phishing attempts: check the sender's actual email (often it's off by a letter or from a weird domain), beware of urgent language and requests for sensitive info, and don't open attachments or links from unknown senders. Hover over links to see where they really lead (on a computer, you can see the URL preview). If something looks even slightly off – verify via another channel. That could mean calling the sender on a known number ("Hey Supplier X, did you really send this PDF?") or checking the company's official website rather than a link in the email. Never send sensitive info like passwords or bank details over email on request – legitimate companies will not ask for your password via email. Also be cautious with attachments – a common scam is a seemingly innocent Word/Excel file that actually contains a macro virus. If you aren't expecting a file, confirm with the sender.

When browsing the web, stick to well-known sites for downloads; avoid pirated software and crack sites – they are often booby-trapped with malware. If a pop-up suddenly says "Your computer is infected, click here to clean" – that's likely a scam. Use modern browsers (Chrome, Firefox, Edge) as they have built-in phishing and malware protections – keep them updated. Consider adding an ad-blocker extension; it can reduce risk of malvertisements (ads that lead to malware). And absolutely avoid plugging unknown USB drives into your computer – this is a real-world trap where attackers drop infected USB sticks in parking lots hoping someone will pick up and insert out of curiosity (it works!). If you find a random USB, better to destroy it than plug it in.

- **Data Protection:** Despite all precautions, things can go wrong – that's why backups are your safety net. Follow the 3-2-1 rule: keep 3 copies of important data (production data + two backups), on 2 different media (maybe one in cloud, one on an external hard drive), with at least 1 offsite (could be the cloud or even a USB kept at home). This ensures that even if one backup fails or your office is inaccessible, you have another. Automate backups so it doesn't rely on someone remembering. There are many cloud backup services affordable for SMEs, or you can use built-in OS tools to schedule backups to an external disk. The key is to also test your backups periodically – make sure you can actually restore files and that the files aren't corrupted. A backup that can't be restored is no backup at all.

Consider encrypting sensitive data, especially on portable devices and in backups. Full disk encryption is built into most operating systems (BitLocker for Windows, FileVault for Mac – just turn it on). That way, if a laptop or external drive is stolen, the thief can't read the data without the password. For cloud backups, many services offer encryption – use it, and keep the encryption key/password safe. Furthermore, control who can access what data internally. Not every employee should have the entire customer list or all financials on their laptop. Use access controls (even simple ones like network shared folders with permissions, or Google Drive's sharing settings) to limit access based on role. This also helps minimize damage if one account is compromised.

Finally, clean up old data securely. If you have old hard drives, don't just toss them – wipe them with secure erase tools or physically destroy them (drill through the platter) if they had sensitive info. For paper records, invest in a cross-cut shredder – it's a simple way to thwart dumpster divers looking for confidential info in trash.

These essential practices form a strong foundation. According to a Stanford University study, 88% of breaches could be traced to human error – things like misconfigurations, use of default passwords, falling for scams. Our checklist directly addresses those common errors. It's not high-tech: it's like locking doors, setting alarms, and teaching everyone not to open the door to strangers.

And just like basic hygiene prevents the majority of illnesses, basic cyber hygiene can prevent the majority of cyber incidents that plague small businesses.

Building a Security-Aware Culture

Earlier we noted that humans are often the weakest link. However, they can also be your greatest defense if they're informed and vigilant. Creating a security-aware culture means making cybersecurity everyone's responsibility and second nature in daily work. Here's how even a small business can do that:

- **Tone at the Top:** If the boss prioritizes security, employees will too. This doesn't mean you need to become paranoid – it means demonstrating good practices yourself (e.g., you use MFA, you don't ask employees to email you passwords in plain text, etc.) and talking about the importance of security in meetings. When staff see management taking it seriously – not as a burden but as essential to business – they'll adopt the mindset. For instance, a small CEO including a quick "security tip of the month" in town-hall meetings sets the tone that it matters.
- **Regular Training & Reminders (Keep it Practical):** Attention spans are short. Rather than an annual long lecture on cybersecurity (which everyone will forget), do short, frequent doses. For example, start a habit that once a month you circulate a one-page bulletin or a short video link on a security topic: one month "How to spot phishing emails" (with screenshots of real examples), next month "Creating strong passwords," another month "Secure use of WhatsApp and social media." Government bodies like CERT-In and many banks produce easy-to-read advisories for the public – you can reuse those for internal awareness. Additionally, consider conducting fun drills: one company sent a fake phishing email to all employees to see who clicks – then instead of punishing clickers, they turned it into a game and learning moment by announcing "X% of us fell for this – here's what gave it away, let's do better." Some may find that sneaky, but it's effective if done in good spirit and not naming-shaming individuals. Encourage employees to share if they encounter something suspicious – create a culture where reporting potential security incidents or mistakes is encouraged, not punished. If someone loses a USB or clicks a bad link, you want them to immediately say so (so you can mitigate), rather than hide it out of fear. Thank employees who speak up about security concerns or who spot phishing attempts and alert the team. Positive reinforcement goes a long way.
- **Implement Simple Policies and Lead by Example:** Develop a basic cybersecurity policy or at least a set of dos and don'ts. It need not be legalese – a one-page "Cyber Rules" that covers essentials: e.g.,
  - "Don't reuse work passwords, don't plug unknown USBs, verify requests for payments, etc." (we've essentially outlined these in prior sections). Distribute it, discuss it in a meeting, and most importantly, management should follow it too. If the policy says "Encrypt your laptop hard drive" or "Use company cloud storage for work files instead of personal email," the leaders should be doing the same. Policy isn't effective if it's just on paper – bake it into procedures. For example, incorporate a security checklist into onboarding ("New joiner gets password manager set up, MFA enabled, reads the cyber rules, and signs off understanding them").

- **Encourage an Open, Non-Blame Culture:** Cyber incidents are often treated with blame, which causes people to hide them. Flip that around. Make it clear that if something happens (they clicked a bad link, accidentally sent something to the wrong person, etc.), the priority is to inform and fix, not to blame. Of course, there's accountability, but first and foremost you want honesty so you can respond. When employees report near-misses (like "I got this weird email and almost fell for it"), commend them for reporting and use it as a learning example for all. You might even institute something like a "Security Champion of the Month" – someone who reported a phish or suggested a security improvement gets a small reward (even a shout-out or a gift card). This motivates engagement.
- **Make Security Part of Everyday Discussions:** Bring up security in team meetings when relevant. E.g., project planning – "We're going to collect customer data with this new app, how do we secure it?" or "We plan to use a new SaaS tool, let's check if it has proper security and backup options." Normalizing this means everyone from HR to Sales thinks about protecting data as part of their job, not just IT's job. If a staff member finds a strange USB in the parking lot and because of awareness training they don't plug it in but instead hand it to IT – celebrate that decision.
- **Learn from Incidents (yours or others):** When something notable happens, use it as a case study (internally, if it happened to you, or externally if you read about an SME getting hacked in the news).

- Without naming any employees, discuss in a blameless way what went wrong and how to avoid it. For instance, "Last week we had a virus infection via an old unpatched software. We've cleaned it and updated systems – learning: we must keep software updated. We'll all need to restart computers at end of week for patching." This reinforces lessons and shows a commitment to improvement.

Building a culture doesn't happen overnight, but these small steps accumulate. Remember, technology defenses can fail, and people are truly the last line of defense. You want those people to be alert, informed, and empowered to act (or not act, in the case of not clicking something bad!). One encouraging metric: a Mimecast study found that consistent awareness training reduced unsafe click rates by 60% or more over a year. People can learn and improve.

Cybersecurity for Cloud and SaaS Tools

Chances are, your business uses at least some cloud or SaaS services – be it Google Workspace for email, Microsoft Teams, an online CRM, or even a cloud server on AWS. While many security basics apply equally to cloud (passwords, MFA, etc.), there are special considerations when your data and operations live on third-party systems:

- **Shared Responsibility (Know Your Part):** As mentioned in the cloud section earlier, cloud providers secure their infrastructure, but you must secure your usage of it. For example, Microsoft will keep Office 365's servers safe, but if you set weak passwords or share files publicly by mistake, that's on you. Always configure cloud services with security in mind: set strong admin passwords, use MFA for admin panels, limit who can see what (most SaaS have role-based access – use it so that an intern isn't suddenly downloading all customer data because they have full rights). Understand default settings – many SaaS are secure by default, but some might have convenience features that lower security (like link-based sharing for files). Tweak settings to balance security and need. E.g., on Google Drive or Dropbox, prefer sharing with specific people's emails rather than open links whenever possible.
- **Secure Your Cloud Accounts:** Treat account logins to important SaaS (e.g., billing software, domain registrar, cloud server console) like keys to the kingdom. Use unique, strong passwords and enable MFA on all of them. Often, compromising an admin's cloud account is more devastating than hacking an on-prem server, because that account can access a lot from anywhere. Also, when staff leave, promptly remove their access to cloud tools (don't forget these in your HR offboarding checklist!). Many breaches happen weeks after someone left and their account was still active. If you use OAuth (log in via Google/Microsoft to third-party apps), review those connected apps periodically and revoke ones not needed – those connections can be entry points too if not monitored.
- **Cloud Data and Privacy:** If you use SaaS to store customer data, ensure the SaaS provider has proper security and privacy policies (most reputable ones do). Stick to well-known providers when possible – for example, rather than using a random free form builder that stores data who-knows-where, use trusted ones or host your own. If you must use a niche cloud service, do a bit of homework: are they HTTPS secure? Do they have two-factor auth available? Are they compliant with regulations you might fall under? As a small business, you may not run a full vendor risk assessment like big companies do, but at least look for red flags (zero info about security on their website, or very poor reviews about data handling). Remember, your clients trust you with their data, even if you in turn put it on a cloud – you're still accountable for its safety.
- **Avoid "Shadow IT" Cloud Usage:** Shadow IT is when employees sign up for online services with company data without formal approval (often just to get a job done). For example, a marketing employee might upload a list of leads to a free email blasting tool to send a newsletter. They mean well, but maybe that tool has poor security or will misuse the data. Encourage a policy where employees should clear use of new SaaS tools, especially if it involves sensitive data. Not to be bureaucratic, but to assess risks. Provide approved tools to meet common needs (e.g., if file sharing is needed, ensure everyone knows to use the official OneDrive/Google Drive instead of random file-sharing sites). It's about creating an environment where employees don't feel they have to go rogue to get work done – offer secure solutions and guidelines.

- **Backup Your Cloud Data:** Cloud services often have great uptime, but they are not immune to data loss (could be due to user error or a rare bug). Many SaaS assume you will have backups of critical data. For instance, if you delete a bunch of contacts in your cloud CRM by accident and only realize a month later, the service might not retain them that long. For key data, either export periodic backups or see if the SaaS offers add-on backup options. Some third-party services specialize in backing up SaaS data (like backing up your Office 365 emails to a separate cloud). Consider the cost vs. risk; small businesses may not need all data backed up, but think about which data would be irreplaceable if the SaaS closed or account got corrupted – back those up (e.g., export your customer list from an invoicing system to Excel every so often and keep securely).
- **Account Monitoring and Alerts:** Many cloud services can send alerts for suspicious activity. For example, Google will alert if there's a login from a new device; Microsoft 365 can alert an admin if there are unusual login attempts. Make sure these notifications go to someone responsible (not to a mailbox no one checks). Also, check account activity logs regularly if available – an admin can review recent logins or changes. This can catch unauthorized access early. Cloud admin consoles often show if someone enabled forwarding on an email (a trick attackers use to covertly get copies of emails) – reviewing settings like that can uncover breaches.
- **Vendor Security Features:** Use the security features your cloud/SaaS vendor provides. E.g., Geo-restriction – if your business works only in India, some cloud accounts let you block logins from other regions. IP whitelisting – some services allow access only from your office IP or via VPN. Device management – if using Google Workspace or Microsoft 365, you have options to enforce screen locks or wipe a lost phone that was connected. These are powerful and often underutilized by SMEs. They might require a premium tier, but weigh the cost vs. benefit for your situation.

In essence, don't assume the cloud provider handles everything. They give you the tools (and a secure base), but you must wield those tools correctly.

A cloud account is like a powerful car – built with safety features, but if you speed recklessly or leave it unlocked, accidents can happen. The major advantage is cloud platforms often log and guide a lot – use their documentation and security checklists (AWS, Azure, Google all have small business security guides).

Many MSMEs actually improve security by moving to reputed cloud services (since those have teams focusing on security 24/7, which a small business cannot afford). But that's true only if you configure and use them properly. So, set up your cloud services with the same (or more) care as you would an on-prem system. And whenever you start using a new SaaS, take 5 minutes to visit its settings page – often you'll find options to improve security (turning on MFA, enabling encryption, setting up auto-logout after inactivity, etc.).

Incident Response: What To Do When Things Go Wrong

Despite best efforts, you should be prepared for the scenario: "What if we get hacked or face a cyber incident?" Having an incident response plan is critical. It's like a fire drill – you hope to never need it, but if you do, you'll be grateful you planned it. Here's a simple step-by-step playbook tailored for small businesses:

1. Don't Panic – Assess the Situation: When a potential incident is discovered (e.g., ransom note on screen, antivirus alert of a serious threat, a system is behaving oddly, or you suspect a data leak), take a breath. Panicking can lead to knee-jerk reactions like wiping evidence or worsening the issue. Try to identify what's affected – one computer? whole network? a specific account? For instance, if one PC shows ransomware, it might be a localized infection – check if shared files are encrypted or just that PC's files. Quick assessment helps decide next steps.

2. Isolate Affected Systems: To prevent spread, disconnect compromised devices from the network immediately. Unplug the Ethernet cable or turn off Wi-Fi. If a server is under attack, consider taking it offline. If malware is spreading, isolating machines can save the rest. Also, change the password of any accounts you suspect might be compromised (do this from a secure device). For example, if you realize an email account was hacked (friends say they got weird emails from you), log in from another clean device and change its password and revoke all active sessions.

3. Communicate Internally (and Externally if needed): Inform key people in your organization. In a small company, that might just be the owner/CEO and the IT support provider. Make sure employees know something's wrong so they can avoid using the affected systems – e.g., "Our file server might be infected, do not use it until further notice." If client data is involved, you will eventually need to communicate with clients – but preferably after initial containment (unless regulation forces very quick disclosure). However, do notify any external IT/security help early – if you have a contract with an IT firm, call them ASAP. And if you suspect a major breach of personal data, consider informing legal counsel or at least start drafting a notice as regulations may require informing authorities or affected individuals within a certain timeframe (India's laws are evolving; globally GDPR requires 72h notice to authorities for serious breaches).

4. Contain the Damage: This overlaps with isolation but also means disabling any breached accounts, blocking malicious IPs at your firewall, etc. If ransomware is actively encrypting files, after isolating, try to halt it (shutdown the PC). If a virus outbreak, run antivirus scans on all potentially impacted systems (from safe mode or using a bootable scanner). If data was stolen (like you find evidence that your database was exfiltrated), immediately secure that system (take it offline, change credentials, apply patches). Basically, stop the bleeding. In some cases, it might mean temporarily shutting down parts of operations (better a short halt than ongoing damage).

5. Eradicate and Recover: Once contained, work on removing the threat and restoring operations. Remove malware (use reputable anti-malware tools, or wipe/reinstall the machine if needed). For ransomware, identify if you have clean backups – if yes, you can start restoration (after cleaning the malware). Do not pay the ransom unless absolutely last resort – there's no guarantee and it fuels more crime. Many times, data can be restored from backups (even if a week old, better than nothing). If backups fail, there are decryption tools for some ransomware if keys have been found (NoMoreRansom.org is a good resource). For compromised accounts, after password resets, check settings (hackers often set forwarding rules on emails or leave backdoor users in systems – remove those). When recovering, bring systems back gradually and monitor them closely. Keep an eye for any continuing suspicious activity – it's not unheard of that attackers re-enter if all passwords weren't changed or root cause not fixed.

6. Document and Learn: As you handle the incident, log what happened – dates, times, what was affected, actions taken. Not only is this useful if you need to report it (to insurance or regulators), but it becomes a learning document. After things are stable, hold a short post-mortem meeting: How did this happen? What worked/didn't in response? Plug the gaps – e.g., "Malware got in because we hadn't patched software X – let's schedule regular updates" or "We discovered our backups hadn't been tested and were failing – let's fix that process." This is crucial: many companies suffer repeat incidents because they patched zero of the underlying issues.

7. Notify as Required: If personal data of customers or employees was breached, you may need to notify them and possibly a government authority (as per applicable law). The communication should be honest and outline what data was involved and what you are doing about it. For example, if customer credit card numbers were exposed (which can happen if your payment system was breached), you'd advise them to monitor their card statements or reissue their cards. If an attack could impact others in your supply chain (say you send a virus to clients unwittingly), inform those partners so they can check their systems. Timeliness matters – hiding a breach often causes bigger backlash than the breach itself.

8. Consider Law Enforcement: For serious breaches (like significant financial fraud or a deliberate targeted attack), you can file a complaint with the local Cyber Crime cell or through the national cybercrime reporting portal. They might or might not be able to actively help (resource constraints, etc.), but having it on record is useful. Sometimes, law enforcement is aware of larger patterns and can connect your case as part of breaking a syndicate, etc. Also, if you have cyber insurance, prompt notification is required to make a claim and they often assign an incident response team to assist.

The overall principle is: time is of the essence. Quick action can prevent an incident from becoming a disaster. For instance, catching a ransomware while it's encrypting one PC and cutting it off could save your servers from getting hit. Or noticing an email account breach and resetting it can stop a fraudulent payment that the attacker was trying to set up. That's why incident response plans should be rehearsed. Even a tabletop exercise ("What would we do if…") with your team can reveal weak points (maybe nobody knows who has the admin login to the router – you realize you should store that centrally).

Small businesses sometimes think "we'll deal with it if it happens." But in the heat of the moment, confusion can reign – having pre-thought steps, and perhaps a small "emergency contact list" (IT support's number, cyber insurance's hotline, key vendors, etc.) can save precious minutes and reduce damage.

Cybersecurity on an MSME Budget

We've covered a lot of ground and you might wonder: what will all this cost? The good news is, many essential cybersecurity measures are low-cost or even free – it's more about effort and discipline. Let's break down some no-cost vs. some worthwhile investments for a modest budget:

What you can do for free or almost free: - Training and Policy: Creating a security policy or sending out tips costs nothing except your time. Plenty of free resources (government CSIRTs, YouTube, blogs) provide content you can adapt. A monthly in-house security email or 15-minute talk in a meeting is free and effective. - Strong Passwords & MFA: Using a password manager might cost a little (some are free for basic, or a few hundred rupees per year for pro versions – peanuts compared to losses it prevents). Enabling MFA is free on almost all platforms (just use an authenticator app or receive OTPs). This gives huge security payback for zero cost. - Software Updates: Keeping software updated is more about process than money. Most updates are free. It's about scheduling it. Same with enabling built-in firewalls and encryption on devices – these features are included in modern OSes, just turn them on. - Antivirus: There are free AV options (like Avast Free, or Windows Security which is built-in and top-tier these days). For many MSMEs, that plus good browsing habits is enough. If you handle highly sensitive stuff, you might opt for a paid suite with extra features, but basic AV is attainable without spending. - Backup Data Using Existing Tools: You can use Google Drive or OneDrive (the free quotas or affordable plans) to regularly copy important files (just be mindful of encryption if sensitive). Or schedule Windows' built-in backup to a spare hard disk. Many SMEs underutilize storage they already have – e.g., that USB drive lying around can be a monthly backup disk (just store it safely offsite afterwards). - Network Security with Existing Hardware: Most offices have a basic router from the ISP. You can log in to that (free) and set a strong admin password and Wi-Fi key. Maybe segment a guest Wi-Fi network (many routers support a "guest network" isolation – check settings). Using a free DNS filtering service (like Cloudflare's 1.1.1.2 for malware blocking or Quad9) at the router can add a layer of malicious site blocking enterprise-grade, at no cost. - Use Free Tier Security Services: Some vendors offer free security assessments or tools for small businesses. For example, there are free phishing test emails services (Sophos Phish Threat trial, etc.), free vulnerability scanners for websites (like Qualys's community edition). Take advantage of these to find holes without paying consulting fees.

What's worth spending on (if budget allows): - Advanced Threat Protection: If you can spend a bit, upgrade email to include phishing protection and spam filtering (often part of business email packages). For example, Microsoft 365 Business Premium includes Defender for Office 365 which filters malicious attachments and links. Google Workspace has builtin phishing protection but higher tiers add admin controls. These might add a few hundred rupees per user per month but can be worth it to drastically reduce risky emails reaching inboxes. - Paid Antivirus/Endpoint Security: Paid solutions (like Kaspersky Small Business, Norton, etc.) often have centralized management – useful if you have 10+ PCs to ensure all get updates and any infection on one alerts you centrally. Some also include features like web filtering, device control (blocking unknown USB devices), etc. These suites could be ₹500-₹1000 per device per year. If that's affordable, the extra features and support can be nice. If not, free AV plus careful practices can suffice. - Managed IT Services or Consultants: If you lack any IT specialist, consider contracting a local IT service company to do a security audit and basic hardening for you – many offer an SME package (they might come and ensure all your systems are updated, set up a firewall, train staff, etc.). The cost might be a fixed project fee or a monthly retainer. Even a one-time audit (few days of work) could be ₹20k-₹50k depending on scope, but it might reveal glaring issues and fix them before a hacker finds them. Similarly, having an IT firm on call (like an AMC – annual maintenance contract) might cost some thousands per month but then you have pros to call during incidents, which can save you massively by quick containment. - Cyber Insurance: This is relatively new but insurers have started offering cyber risk policies even to small businesses. The premium might range widely (₹10k to ₹50k or more annually) depending on coverage (which can include incident response costs, legal expenses, notification costs, even ransom reimbursement in some cases). If your business would struggle to financially survive a major breach or downtime, insurance can be a safety net. Be sure to read what's covered and what conditions (they often require you maintain basic security practices – they won't pay if you were grossly negligent like no passwords or something). - Hardware Upgrades: Consider investing in some security hardware if appropriate. For example, a proper business-grade firewall/router (~₹15-30k one-time) can provide stronger network defense than the ISP router (intrusion prevention, content filtering). If your budget is tight, this isn't first priority, but as you grow it's worth it. Another example: encrypted USB drives for transporting data (they cost a bit more but if you regularly carry sensitive files, buy a couple of hardware-encrypted pen drives).

- Upskilling Staff: Pay for an employee (maybe your IT point person or whoever is tech-savvy) to attend a cybersecurity workshop or get a basic certification. Investing in human capital can yield improved security posture. There are low-cost online courses (some under ₹500 on platforms during sales) that someone could take and then implement learnings internally.

Prioritizing spending: It depends on your risk profile. If you handle a lot of customer PII or financial info, spend more on things like encryption, DLP (data loss prevention) tools, and insurance. If your main risk is ransomware halting operations, invest in robust backup solutions (maybe a cloud backup service which costs monthly per GB) and perhaps a managed detection and response service (some companies offer SMB-friendly 24/7 monitoring of your systems for a fee – might be pricey, but it's like a security guard for your network). If phishing has historically been an issue, upgrade email security and do a paid phishing simulation campaign until the team improves (some vendors charge per user for simulated phishing and training modules).

Remember, many security measures cost far less than the potential damage of an incident. A ₹5,000 expense on security could prevent a ₹5 lakh loss. Of course, no one has unlimited budget, so cover the basics free stuff first (they reduce most risk). Then address the biggest gaps or most likely threats for your business with targeted spending. Keep receipts and note improvements – sometimes this can also reduce insurance premiums or satisfy client requirements.

The bottom line: you don't need a big-city bank's security budget to significantly improve your cybersecurity. Smart, focused investments of time and a modest amount of money can dramatically lower your risk. As one stat showed, 95% of SMB cybersecurity incidents cost between $826 and $653,000 – a wide range due to severity; spending even a small fraction of the upper end on precautions is well worth avoiding even the lower end of those incident costs.

Future Trends & New Risks

The cybersecurity landscape is ever-evolving. Small businesses don't need to chase every hype, but being aware of emerging trends helps you stay ahead of new risks:

- **AI-Powered Attacks (and Defenses):** Just as you can use AI to help your business, attackers can use AI to craft smarter malware and more convincing scams. For instance, deepfake technology can create fake voices or videos. Already, cases occurred where fraudsters cloned a CEO's voice to trick an employee into transferring funds. In the future, a scam call might sound exactly like your manager or a VIP client, complete with the right accent and tone, thanks to AI. It will require a shift from "voice = verify" to perhaps code phrases or call-back verification for sensitive requests. Similarly, AI can generate phishing emails that are grammatically perfect and contextually relevant (maybe scraping your social media to personalize a message). The age of obvious "Dear Sir, I is needing your help kindly" emails is ending; expect phish that read like a genuine email from a colleague, making them harder to spot.

On the flip side, AI is also bolstering defense – tools that detect anomalies using machine learning or email filters that flag content likely written by AI rather than a human (some orgs use AI to detect AI-generated phishing). The arms race is on. Practical tip: remain cautious even if a communication seems legit; double-check unusual requests especially involving money or data, even if the medium (voice/video/email) seems authentic. "Trust but verify" will evolve to "Verify, then trust" by default.

- **Zero Trust Architecture:** This phrase means exactly what it says – trust no one by default. Traditionally, companies had a secure perimeter and inside it, things were trusted (like internal network devices). Zero Trust says assume breach and verify each action. For a small business, adopting full zero trust might be overkill, but adopting its mindset can help. Concretely, it means segmenting networks (so an infection on one PC doesn't automatically spread everywhere), enforcing re-authentication for sensitive actions (even if someone is already logged into the VPN, maybe a finance app asks for MFA again to approve a fund transfer), and not assuming insiders are clean (monitor internal traffic for malicious signs too). As more solutions come that make zero trust easier (like cloud-based secure access service edge – SASE – offerings that even SMEs can use to secure remote work), consider them. We already gave an example: requiring VPN for any access to internal resources is a zero trust principle ("don't trust that just because they're in office, they're legit"). Another: if you have an internal file share, maybe require login even when on the office LAN, not open to everyone.
- **Expansion of Digital Payments and the Fraud Around It:** India leads in real-time digital payments (UPI, etc.). With 12+ billion UPI transactions a month, scammers are all over this – from fake UPI payment screenshots to social engineering UPI PINs.

- Every small business now dealing with UPI or wallet payments should educate staff on how these systems actually work (e.g., that receiving money never requires you to enter your PIN – a common scam is sending a "payment request" that novices confuse for receiving). The same goes for card-on-delivery scams (asking your delivery agent to swipe a card on a fake POS that actually clones it). As more commerce moves online (share of e-retail in India set to double by 2030), expect more fraud attempts. Keep up with the latest scams – make it a topic in your awareness training. If you run an online storefront, be vigilant for fraud orders (e.g., large order from a new customer overseas, etc. – possibly use fraud detection tools or only ship after payment clears). Digital payments are great for efficiency but require a level of digital literacy to handle safely. The more your business transacts online, the more you should invest in securing those channels (like using payment gateways with built-in fraud checks, enabling two-factor for banking, etc.).
- **New Regulations and Legal Requirements:** Governments are paying attention to cybersecurity for small businesses. India's Data Protection Act will impose obligations even on SMEs regarding personal data handling (like obtaining consent, reporting breaches). Sector regulators (RBI for fintech, IRDAI for insurance brokers, etc.) are pushing down cyber requirements to even smaller entities. For example, IRDAI recently asked small insurance entities to implement basic cyber measures and will audit them. Also, large companies are flowing down compliance to vendors (e.g., requiring ISO 27001 certification or adherence to certain frameworks as a prerequisite to contract). It's plausible that in a few years, having a baseline cybersecurity posture will be like having a PAN or GST – just part of business due diligence. Smart SMEs might preempt this by aligning with a well-known standard (maybe not fully certifying, but following, say, NIST CSF or the basic tenets of ISO 27001). This can also be a market differentiator: "Your data is safe with us; we follow XYZ best practices and have insurance." We already see this in tenders – some PSUs ask about bidder's cybersecurity.
- So, future-proof by formalizing some of what you do (document policies, maybe do an annual external security audit and keep that report to show customers if needed).
- **The "Cyber-Covid" – Increased Remote Work Risks:** The pandemic forced remote work on many, and that hybrid model is here to stay. That expands the attack surface from office networks to home routers and personal devices. Attackers leapt on this (e.g., phishing users with fake VPN login pages, exploiting people on home Wi-Fi with default passwords, etc.). Businesses responded by using more cloud and collaboration tools – which is great, but requires our discussed controls on cloud security and user training to not mishandle data. Ensuring secure configuration of remote access (using reputable remote desktop software or VPNs with MFA, etc.) is key. If remote work will continue for your business, invest in securing it – maybe stipend for employees to upgrade to a router that supports better security, or at least guide them on changing default Wi-Fi passwords. Provide them with security software licenses if needed for personal devices they work on. Essentially treat each remote location as an extension of your office security-wise.
- **Cyber Insurance Evolution:** As more SMEs claim incidents, insurers are adjusting. Premiums might rise, or certain high-risk behaviors will void claims (e.g., if you didn't patch a 3-year-old vulnerability, they may not pay for that breach). Insurance might even become a requirement by partners (like some B2B clients might require you carry cyber insurance if you deal with their data, to ensure you can cover breach costs). Stay informed on this front if you consider insurance, and definitely read the fine print on security obligations in the policy.
- **Threat Landscape Change – More Targeted Attacks on SMEs:** Traditionally, many cyberattacks on SMEs were scattershot (mass phishing, broad malware). Now, organized cybercriminal groups have realized SMEs can be lucrative and often more vulnerable than big companies. There's evidence some ransomware gangs now specialize in hitting smaller companies and demanding smaller ransoms (say ₹5-10 lakh) knowing the business might actually pay as they don't have big IT teams to recover quickly. It's sort of "mid-volume, mid-value" crime vs. going after one giant target. This means the threat level for SMEs is actually rising. Don't assume "we're too small to be noticed." As noted, 43% of all breaches in 2021 were on small businesses. Adopting the measures we've discussed is not overkill; it's timely.

In essence, cybersecurity for small businesses must become a continual effort, not a one-time project. Keep an ear out for news of new scams (subscribe to a security newsletter or follow Cyber Dost – an initiative by Indian govt on Twitter – they share current scams).

Adapt your defenses as needed. For example, if deepfake voice scams become common, implement a verification step for any financial transaction requests that come via voice-only.

The future will bring new gadgets (IoT everywhere – think smart locks, security cams) which help business but also need securing (change those default passwords!). It will bring more reliance on data (thus more target on data). But with the right mindset – proactive, informed, and adaptive – even a micro enterprise can navigate it safely.

Checklists & Sidebars

Cyber Hygiene Checklist for Small Businesses: (Use this as a quick reference to ensure you've covered the basics.)

1. Software Updates: All PCs, servers, and devices have automatic updates enabled. Key software like operating systems, browsers, and antivirus are set to update regularly (at least monthly).

2. Strong Passwords: No default or blank passwords on any device or account. All staff use strong passwords (preferably 12+ characters or passphrases). Consider using a password manager to generate and store unique logins.

3. Multi-Factor Authentication: Enabled for all important accounts (email, VPN, banking, cloud admin accounts, etc.). Staff are trained to use authenticator apps or carry tokens as needed.

4. Secure Wi-Fi: Wi-Fi uses WPA2/WPA3 encryption with a strong passphrase (not something easily guessed). Router admin interface has a non-default password. Guest network is isolated from business network.

5. Endpoint Protection: Every computer has anti-virus/anti-malware active and updating. Firewalls (built-in OS ones or network firewall) are turned on to block unwanted connections.

6. Data Backups: Important data (documents, databases, emails, etc.) are backed up regularly following 3-2-1 (multiple copies, different media, one offsite). Backups are tested (do test restores periodically). Backup drives or cloud storage are secured (encrypted or kept safe).

7. Access Control: Each employee has their own user accounts – no sharing of login credentials. Access to files and systems is given on a need-to-know basis (least privilege). Administrator accounts are limited to those who need and used only when necessary.

8. Secure Configuration: Defaults have been changed (e.g., admin passwords on devices, unnecessary services disabled). Any cloud services are reviewed for security settings (sharing permissions, etc. set appropriately).

9. Email Caution: Spam filters are on. Staff know how to spot phishing. No sensitive info (passwords, OTPs) is ever sent over email/plain text. When in doubt, verify sender's identity via alternate channel.

10. Device Security: All company laptops have full-disk encryption enabled and lock automatically after a few minutes idle. Mobile devices used for work have at least PIN lock and, ideally, remote wipe capability. Lost or stolen devices are reported immediately so passwords can be changed and remote wipe used if possible.

11. Physical Security of Data: Important documents are shredded before disposal. Old hard drives are securely wiped or destroyed. Server rooms or network cabinets are locked to prevent unauthorized access or tampering.

12. Incident Plan: There is a simple, understood procedure for incidents. Key contacts (IT support, cyber insurance, management) are listed. Staff knows to report incidents immediately without fear. Data breach response plan (who to notify, how to isolate systems) is written down.

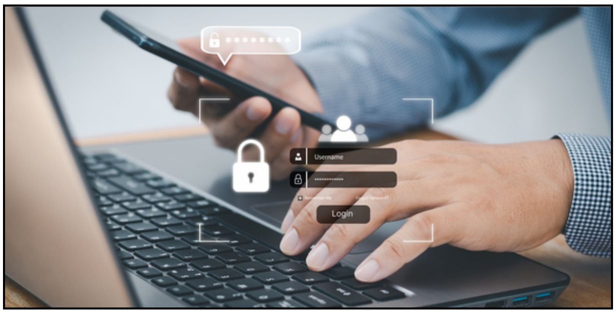
13. Continuous Awareness: Security training or reminders happen regularly (e.g., monthly tips). Employees are encouraged to ask questions and stay vigilant. New hires receive security orientation.

(Run through this checklist every quarter to ensure things haven't slipped.)

Questions to Ask Your IT or Security Vendor: (If you outsource IT or are evaluating a security product/vendor, use these questions to gauge their effectiveness.) - "How do you ensure our systems stay updated and patched?" – Listen for an answer about a routine or automation (e.g., "We apply critical patches within 48 hours, and all systems are set to auto-update weekly"). - "What protections do you provide against phishing and ransomware?" – A good vendor might mention email filtering, user training, backups that are ransomware-proof, etc. If they just say "we install antivirus," that's not comprehensive. - "Will you help us develop an incident response plan and be there if an incident occurs 24/7?" – Important to know their support hours and commitment. Cyber incidents don't always happen 9-5. - "How do you secure remote access to our systems?" – They should talk about VPNs, MFA for admin access, disabling risky remote ports, etc. If they shrug and say "remote desktop is open with password login," that's a red flag. - "What kind of backup solutions and disaster recovery do you implement?" – Listen for 3-2-1 backups, offsite storage, test restores. If they say "Uh, we have RAID on the server" – that's not a backup (RAID doesn't protect against deletion or ransomware). - "How will you help protect personal data and comply with regulations like data protection law?" – They should be aware of basic data privacy principles (encryption, access logs, consent management if applicable). If you get blank looks, they might not be keeping up with compliance needs.

- "Can you provide references or examples of how you handled a cyber incident for a client?" – A vendor who has seen action will have a sanitized story like "Client X got hit with ransomware, but we had them restored from backup in 4 hours." That inspires confidence. If they have no such story, maybe none of their clients had issues (good) or they're inexperienced (not so good). - "What security certifications or frameworks do you follow?" – If they mention ISO 27001, CIS controls, or even just say "We follow industry best practices from NIST," that's positive. It means they have a structured approach. If they brush it off with "Small companies don't need that stuff," be cautious – a methodical approach is valuable regardless of size.

Asking these questions will not only get you useful information but also signal to the vendor that you expect a high standard. Their responses can help you differentiate between a mediocre IT provider and one that will truly strengthen your security.



Conclusion: Make Cybersecurity a Daily Habit

We've covered a lot, from the threats out there to the concrete steps to guard against them. For a small business owner or manager, it might feel daunting – but remember, you don't need to implement everything overnight. Start with the basics: ensure updates are done, use strong passwords with MFA, back up your data. These alone dramatically reduce risk. Then address other gaps gradually, and keep educating your team. Cybersecurity isn't a one-time project, it's like maintenance – an ongoing part of operations, much like bookkeeping or quality control.

The encouraging part is that the most effective measures are not super high-tech or expensive – they're often about consistency and awareness. It's more about mindset than budget. Cultivating a culture where everyone is a bit careful – checking that link before clicking, confirming that request that seems odd – can prevent disaster. One employee noticing and reporting a suspicious email could save your whole business from a major breach.

Make cybersecurity a routine topic: just like you'd review finances or sales regularly, review security. It could be a five-minute blurb in meetings ("No major issues this month, reminder to folks: our helpdesk will never ask for your password, so be wary of any such requests.").

Encourage an atmosphere where if someone makes a mistake (falls for a phish), they report it immediately and it's treated as a learning opportunity, not a personal failure.

Finally, understand that strong cybersecurity can be a business enabler, not a hindrance. In an era where even customers are concerned about their data, being able to say "we prioritize your data's security" is a selling point. PSUs, MNCs, and government organizations definitely favor SMEs that are proactive about security – they've been burned by supply-chain breaches before. By implementing the practices outlined, you're not only protecting what you have, you're also positioning your business as a trustworthy partner ready for the digital economy. According to a McKinsey report, India's e-commerce and digital services boom must be underpinned by robust cybersecurity across even tier-2 and tier-3 city businesses – it's a collective effort and opportunity.

As a small business, you might not stop a nation-state hacker – but the reality is, those actors rarely target SMEs. The threats you face are very defendable with the steps we discussed. It's about covering common entry points and being prepared to respond. With that done, you can focus on growing your business with confidence.

So, as a next step, pick 5 actions from the checklist and do them in the next 30 days. For example: 1) Turn on MFA for email, 2) Install updates on all machines this week, 3) Set up a daily cloud backup for key files, 4) Hold a team meeting on phishing examples, 5) Call your IT support and schedule a security audit. These are doable and will put you miles ahead of many peers. Then keep the momentum – security is a journey, not a destination, but each step greatly reduces risk.

Cybersecurity can seem complex, but its essence is simple: protect your business like you protect your home – lock doors (passwords/MFA), use alarms (alerts/logs), keep valuables out of sight (encrypt and limit access), and be skeptical of unexpected visitors (phishing). Do this, and you'll drastically improve your odds against even the sophisticated threats out there. Stay safe, stay alert, and make cybersecurity a daily habit for you and your team.

CA CMA Sandeep Kumar

President - International Navodaya Chamber of Commerce

E-commerce Expansion: Strategies for Establishing and Growing an Online Storefront, Including Marketplace Integration

Introduction

Why Every Business Needs a Digital Storefront

A few years ago, a small manufacturer of organic spices in Jaipur relied solely on local traders and the occasional expo to sell its products. They were doing okay, but growth was slow. Then in 2024, they decided to list on a major e-commerce marketplace and also set up their own website. Within a year, they were shipping pan-India, their revenue had tripled, and they even started getting inquiries from abroad online. Contrast that with another small business – a handicraft maker who refused to go digital and saw orders decline as large buyers shifted to online sourcing and younger retail customers flocked to digital platforms. These stories illustrate a simple truth: in today's market, having an online presence is no longer optional – it's increasingly critical for growth and even survival.

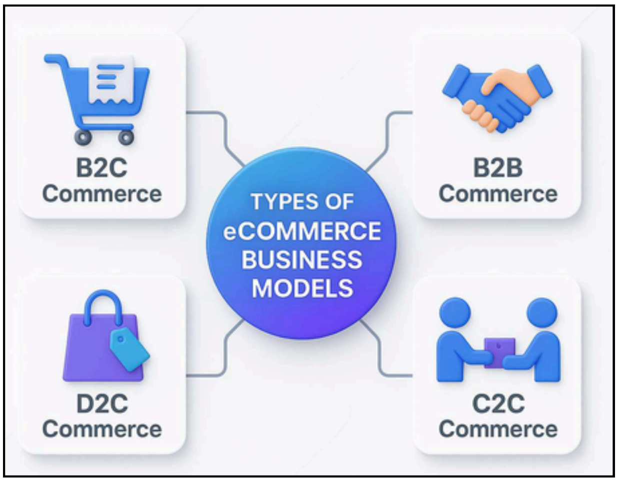
The numbers back this up. Globally, about 21% of retail sales are expected to be online in 2025, up from under 10% just a decade ago. In India, e-commerce accounts for roughly 7-9% of total retail sales as of FY23, and that share is projected to more than double to ~15-17% by 2030. That growth is driven by expanding internet access (over 850 million internet users, of whom only ~20-25% currently shop online – a huge untapped potential), rising comfort with digital payments (UPI now powers ~80% of all retail digital payment transactions in India), and initiatives like ONDC (Open Network for Digital Commerce) aiming to democratize e-commerce for small players.

What does this mean for decision-makers in PSUs, MNC procurement divisions, government supply chains, and MSME owners? It means the ecosystem is rapidly moving online – from PSU procurement portals to B2B marketplaces and consumer platforms. Buyers increasingly expect vendors to have a digital storefront or at least digital catalogs. Government organizations are pushing vendors onto portals like GeM (Government e-Marketplace) for transparency and efficiency. Large corporates manage supplier interactions via online systems.

And consumers – whether urban or in tier-2 cities – are buying online in record numbers (India's online shopper base is expected to rise substantially from the current ~200 million as more of those 850 million internet users gain trust in e-commerce).

In short, having an online storefront is like having a shop in the biggest mall in the world – except this mall is accessible to everyone with a smartphone. It can amplify your reach from local to national or even global. This section will guide you through how to establish and grow your online presence pragmatically: choosing the right model (your own site vs. marketplaces vs. both), laying a solid foundation (products, branding, content), and then marketing effectively (traffic, analytics, customer experience), all with an eye on budget and practical execution for MSMEs and others.

Let's dive into the different e-commerce models first to see which combination might suit your business.



Types of E-commerce Models – From Basic to Advanced

Not all online selling is the same. Understanding the models helps you decide where to invest effort:

- **Direct-to-Consumer (D2C) – Your Own Website:** This is when you set up your own e-commerce website (e.g., a .com or .in site) and sell directly to end customers. Who it suits: Brands or manufacturers that want control over customer experience and data, and have the ability to promote their site. Investment/Effort: Moderate. Tools like Shopify, WooCommerce (a plugin for WordPress), or Wix make it easier – you don't need to code, but you will need to spend on web hosting, a template, payment gateway fees, etc. Possibly you'll need some web design help initially.

- Pros: Full control of branding and presentation, you set your own policies (pricing, shipping, returns), and you directly collect customer info (useful for repeat marketing). Margins can be higher since no marketplace commission. Cons: You have to drive your own traffic (no built-in audience – you'll spend on marketing/SEO for people to find you), and you must handle operational pieces (hosting upkeep, security, integrating couriers) largely yourself. It can start simple though – even a basic site with your catalog and a phone/email order option is better than none, and you can gradually add full cart/online payment features.
- **Marketplaces (Amazon, Flipkart, IndiaMART, etc.):** These are large e-commerce platforms where many sellers list products. Who it suits: Virtually any product seller, especially those who want quick access to a national customer base without building a site from scratch. Also great for MSMEs supplying consumers (B2C) and also for some B2B categories (IndiaMART, Udaan cater to wholesale/B2B). Even government departments browse marketplaces for vendor discovery and price benchmarks. Investment/Effort: Low to start – you can create an account and list products in days. They often have no upfront cost, but they take a commission per sale (ranging ~5% to 20% depending on category and platform). Pros: Immediately tap into millions of shoppers. Trust and payment are handled by the platform (buyers often feel safer on Amazon/Flipkart due to established policies). They provide infrastructure: catalog templates, delivery options (Fulfilled by Amazon, etc.), easy returns for customers (which can be a pro or con). Cons: High competition – your product sits next to competitors and often price is the differentiator. Limited branding – customers may remember buying from Amazon, not from your store name. The marketplace owns the customer relationship (they usually won't give you the buyer's contact info beyond what's needed to ship, and you're often restricted from marketing to them off-platform). Also, rule changes or increased fees on marketplaces are beyond your control.

Example: A handicraft MSME on a marketplace might see good sales during festive season due to the platform's traffic. But if a dozen other sellers add similar items, they might need to cut price or buy ads on the platform to stay visible. Still, marketplaces are an excellent way to get initial volume and market feedback. Many MSMEs use them to supplement their own site. Also, note specialized marketplaces: for instance, PSUs and large cos use B2B ones (like mjunction for steel, or government e-procurement sites). Being present where your buyers are is key.

- **Social Commerce:** This refers to selling through social media channels – like having an Instagram shop, Facebook page store, or even taking orders on WhatsApp.

- **Who it suits:** Small businesses with visually appealing products (fashion, food, crafts) often do well via social channels. Also, businesses that grow through community and engagement (like a boutique building a following on Insta). Investment/Effort: Low technical cost, but high effort in content creation and messaging. Setting up a basic Facebook Store or Instagram Shopping is free (just link to your catalog), and WhatsApp Business app is free and allows a product catalog and quick replies. Pros: Direct engagement with customers, easier to leverage word-of-mouth and virality (a nice product post can be shared widely). It feels personal – some customers prefer messaging the business owner directly. Cons: Managing orders and queries can become very manual as you scale (imagine handling 100 WhatsApp inquiries a day – you might need an employee just for that). Tracking inventory and payments can get messy if you don't streamline (though new tools like WhatsApp Pay and order tracking via messaging are improving this). Also, not all social followers convert to buyers – sometimes you get many inquiries that don't result in sales, which can be time-consuming.

Use-case: A home baker might primarily use Instagram to post cake photos and take orders via DM/WhatsApp. This can work well locally. But if she wants to expand city-wide or nationally (for durable goods like cookies), she might then add a website or join a platform. Social commerce is often a great starting point or side-channel, especially for businesses that thrive on visuals and community (apparel, home decor, artisanal goods). It's also common to see businesses do live commerce (Instagram live sales, etc.), which can mimic the persuasive in-person selling experience online.

- **B2B Platforms and Vendor Portals:** If you supply to PSUs, MNCs, or government, you may need to engage through their specific procurement portals or B2B marketplaces. E.g., GeM (gem.gov.in) is the government's marketplace where even smallest vendors can register and get orders from government buyers. Large companies might have a vendor portal (like SAP Ariba or custom systems) you must log into to receive POs, update invoices, etc. Who it suits: MSMEs that are vendors to bigger entities or who want to become one.

- **Investment/Effort:** The cost is typically just the time to register and comply with requirements (some require digital certificates, paperwork). GeM is free to register but you must have certain documents (GST, etc.). The effort is learning the system's processes. Pros: These platforms can open doors to big contracts that traditionally were hard to access (e.g., a small machinery supplier can directly offer to a PSU on GeM without needing prior connections). Some B2B platforms like IndiaMART generate leads for exporters and wholesalers – a small manufacturer can get bulk inquiries through such a platform listing. Cons: The volume might be unpredictable (listing is one thing, getting chosen is another – you still must be competitive on price/quality). Also, participating in tenders or RFPs on these systems can be complex for those new to it (there's a learning curve dealing with online bidding, digital signatures, etc.). But support is often available (GeM has helpdesks, etc., as they are pushing MSME inclusion).

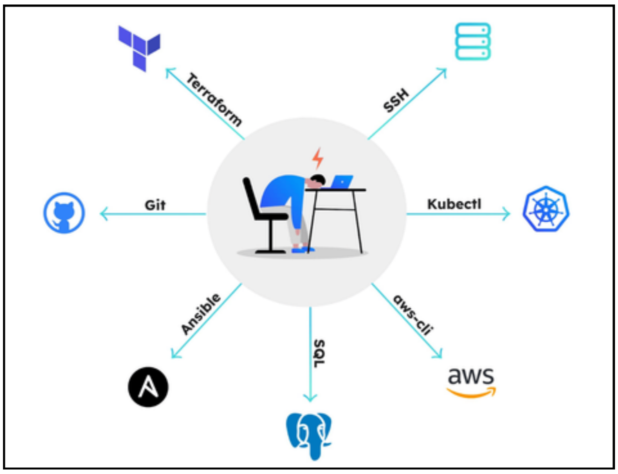
In practice, many businesses adopt a mix: e.g., have their own site for branding and loyal customers, but also list on one or two marketplaces for reach; use social media to drive awareness which funnels either to their site or marketplace listings; and for B2B, maintain a presence on an industry portal or government e-procurement site.

As a decision-maker, consider: - Where are my customers looking? If you sell to young consumers – definitely marketplaces and social media. If to government – GeM. If to corporates – maybe industry B2B platforms or even LinkedIn connections leading to direct deals. - What resources do I have? If you have zero in-house tech, starting on a marketplace or using an easy site builder is wiser than trying to custom-build a fancy site. If marketing budget is thin, piggyback on marketplace traffic first while building your organic social media presence, then later funnel people to your site as brand grows. - What control vs. convenience trade-off suits me? If you're very particular about brand experience (e.g., a premium brand), investing in your own site is a must for that bespoke feel, even if slower sales initially. If your product is more commoditized (like a common electronic accessory), you might just focus on high-volume channels (marketplaces) and not worry much about building a separate brand site beyond maybe a simple catalog page.

Next, let's assume you want to establish some online presence (whichever model). How do you set the foundation right – in terms of products, branding, content – so that when buyers find you, they like what they see and trust you enough to transact?

Setting the Foundation: Products, Brand, and Content

Before you build any online store or profile, get the basics in order:



- **Product Readiness:** Ensure you have a clear, organized catalog of what you sell. This means defining your SKUs (stock keeping units) or service packages clearly. Online, specificity sells. For each product, have details like dimensions, material, variants (sizes, colors), and pricing clearly determined. Also, stock: if you're going online, be prepared for the possibility of more orders. Plan how much inventory you can allocate to online sales and how you'll update stock figures to the platform. Nothing turns a new customer away like placing an order only to be told "actually it's out of stock." If you manufacture on demand, state the realistic lead time and whether you'll accept orders in excess of ready stock. In short, get your product data and supply chain ducks in a row. Digitize what you can: maybe maintain a simple spreadsheet or use an inventory management software (there are affordable cloud ones) to track online inventory. This will help as you expand to multiple channels.
- **Brand Basics:** Online, customers can't meet you or see your shop, so your brand must speak for you. Spend a bit of effort on a decent logo (it doesn't have to be fancy – there are free logo makers or hire a graphic designer for a modest fee). Choose a brand name for your online storefront that is consistent (if your legal name is long or not consumer-friendly, you might use a shorter trade name online – just be careful to not confuse existing customers). Use a consistent color scheme and style in your site or marketplace images to build recognition. Importantly, establish trust signals: highlight quality certifications (ISO, AGMARK, etc.) upfront, mention big clients you serve (e.g., "Supplier to Indian Railways" – that impresses visitors), and any warranties or guarantees (like "100% genuine, or free returns"). If you have been in business X years or are registered with MSME or NSIC, mention that – credibility matters because customers worry if a small unknown online seller is a scam or not.

If targeting international customers, check if your brand name has any negative meanings abroad (just in case – we've seen some funny mishaps in global branding).

Also, secure a domain name that matches your brand if you can (for your own site). It's relatively cheap (₹500-₹1000/year) and even if you aren't making a site immediately, you can use it for professional email (e.g., info@yourbrand.com) which looks more credible than a generic Gmail in business communication.

- **Content – High-Quality Photos, Descriptions, and Policies:** Online, content is your salesperson. Invest time in getting it right:
- **Photos:** Humans are visual. If you sell products, clear, well-lit images are a must. You don't need an expensive camera – today's good smartphone plus some inexpensive lighting can do wonders. Take multiple angles, show the scale (e.g., someone holding the item or wearing it if apparel). For example, on marketplaces a product with 4-5 photos (front, back, close-up of material, in-use context) will convert far better than one with a single grainy image. Ensure your images are not too heavy (for site speed) but high resolution enough to zoom. If you provide a service, include images of your team, your office or equipment, before-after pics if applicable, etc. They provide authenticity.
- **Descriptions:** Write clear, honest, and detailed product descriptions. Avoid only marketing fluff – include factual specs/dimensions, usage instructions, what's included in the package, etc. This not only helps SEO (search engines) but also reduces customer questions. For instance, an apparel seller should list fabric, care instructions, size chart; a gadget seller should list compatibility, technical specs; a B2B equipment seller should list capacity, maintenance requirements, etc. Also, tell the story if relevant – people love hearing "handcrafted by rural artisans" or "our family has made this sweet for 3 generations." It adds a personal touch that big corporations often lack.
- **Pricing and Offers:** Clearly state the price, what it includes (e.g., with GST or shipping). If you have introductory offers or bulk discounts, mention them prominently. Online shoppers often compare – if your price is higher but justified by something (better warranty, free accessory, etc.), point that out. Also, if you cater to bulk buyers, indicate "Contact us for bulk pricing" – you might attract B2B inquiries even through a consumer-facing page.
- **Policies (Shipping, Return, Payment):** Be upfront about how you handle orders. How fast do you dispatch (e.g., "Usually ships within 2 business days")? What are typical delivery times (if you know, say "Delivery in 4-6 days across metro cities")? State your return/refund policy in plain terms: e.g., "We accept returns within 10 days of delivery if the product is damaged or not as described. Please keep packaging, and we'll arrange reverse pickup." Even if your policy is "No returns on custom-made items,"
- stating it clearly avoids future conflict and builds trust (customers feel safer when policies are spelled out rather than hidden). ·Also outline warranty if any, and customer service contact info (email/phone) for issues. Many customers read this to gauge if buying from you is risky or not. A small seller with a clearly stated fair return policy will get more orders than one with none mentioned (buyers fear the worst if nothing is said).
- **Case Example:** A small electronics retailer put effort into content on their new website – for each item, they listed specs, added a short guide on how to use it, and included a testimonial from a customer. They also clearly listed that they offer a 6-month seller warranty. This made their site feel as informative and reliable as a big e-tailer, and customers started trusting them despite them being a new brand.
- **Trust and Social Proof**: If you have any media coverage ("featured in The Hindu" etc.), display their logos or quote. If you have existing customer testimonials or can get some initial reviews, showcase them (people rely heavily on reviews – even one or two genuine positive comments can tilt a decision). On marketplaces, reviews will accumulate (make sure to encourage happy buyers to leave them). On your own site, you can either manually add testimonials or integrate a review plugin. Starting out, you might incentivize first customers with a small coupon for giving feedback (which you can turn into a testimonial quote, with permission).
- **Mobile-Friendly Setup:** Ensure whatever platform you use (your website or the marketplace listing) looks good on mobile. Over 70% of e-commerce traffic in India is via mobile (the country leapfrogged PCs). Most modern website templates are responsive by default, but do test your site on a phone. If using large images or certain layouts, check that text isn't cut off, buttons are easily clickable. This is part of foundation because a clunky mobile experience will drive away the very audience that's shopping online the most.

Setting a solid foundation might take a few weeks of preparation – writing content, doing a photo shoot, setting up accounts and pages, etc. It is effort well spent. Think of it like setting up a physical showroom: you'd decorate, arrange products neatly, put price tags and info – here it's the same principle in digital form.

Once your storefront (be it a marketplace profile or own site or social page) is set up with good content and branding, the next step is to attract customers (drive traffic) and then convert that traffic to sales by providing a great experience and support. We'll cover those in the following sections.

Choosing Technology for the Online Storefront

If you decide to sell through your own website, one of the first technical decisions is which platform or solution to use. The good news: you don't have to build from scratch (and shouldn't, given the robust options available). Here's a rundown of the main approaches:

- **Hosted E-commerce Platforms (SaaS):** These are services like Shopify, BigCommerce, Wix eCommerce, Zoho Commerce, etc. They provide an all-in-one solution – you sign up, choose a template, add products, set up payment and shipping, and you're live. Pros: Very quick to launch (often in days), no coding needed, they handle security, updates, server maintenance. They often have integrated features like product reviews, abandoned cart emails, discount code management, basic SEO tools, etc., which you can turn on easily. For example, Shopify is known for its ease of use and a huge app store to add functionalities (maybe a WhatsApp chat widget or a courier integration). Cons: They charge a monthly fee (Shopify basic is ~₹2000/month) and sometimes a transaction fee. They can be less flexible in terms of deep customization – you fit into their framework (though for most small businesses that's okay). If you ever want to move away, migrating can be a task (lock-in to some extent). Suitable for: Most MSMEs who want a professional store without hiring a developer. I often tell small businesses: if you can budget around ₹20-30k/year, a platform like Shopify can pay for itself in time saved and features.
- **Plugins on Existing Websites (Open-source or CMS plugins):** If you already have a website (perhaps on WordPress for your company blog or info site), you can add e-commerce via plugins like WooCommerce (for WordPress) or Magento (a standalone open-source e-com platform) or others. Pros: Often no software cost (open-source = free, you just pay hosting). Highly customizable – you have full access to code if needed, and many plugins to extend. With WooCommerce, for example, you integrate with Indian payment gateways (Razorpay, PayU) via free plugins, add shipping calculators, etc. Cons: More technical management – you (or an IT person) must handle hosting, SSL certificate, software updates, backups, and security measures. If something breaks after an update, you need to troubleshoot or hire someone. It might be cheaper monetarily than SaaS (since hosting for a small site could be just ₹5k/year and plugin is free), but the hidden cost is maintenance time and potential downtime if not managed well. Suitable for: Businesses with some IT support or those who want a very tailored solution. Also, if you expect rapid scale or need to integrate deeply with other systems, open-source can be tweaked extensively.

Example: A niche electronics retailer chose WooCommerce because they needed a custom bundling feature and wanted direct database access to sync with their offline inventory system. It took more setup time and they had a developer on contract for maintenance, but it gave them exactly the features they needed.

- **Custom-Built Platform:** This means hiring developers to create a site from scratch or using a web framework. Pros: You get exactly what you specify, potentially with unique design and features not available elsewhere. You have full control over the tech stack. Cons: High cost (development can run into lakhs), longer time to launch, and then you must maintain it (if the developer moves on, will you have skills to update it?). For most MSMEs, this route is unnecessary given excellent SaaS and open-source options. Suitable for: Those with very specific needs that off-the-shelf can't handle, or larger enterprises with IT teams. Example might be an online service marketplace with complex logic – but even then, often customizing an existing platform is smarter.
- **Marketplace-Provided Microsite:** Some marketplaces or B2B platforms allow you a "store page" that can function as a mini website (e.g., Amazon Brand Stores). ONDC (Open Network for Digital Commerce) in India is heading towards a model where your product catalog can be shown on multiple buyer apps without you building anything – you just plug into the network via a seller app. Pros: Minimal setup – you piggyback on their ecosystem. Cons: Limited to their ecosystem's reach and features; not a full-fledged independent presence.

- Suitable for: Starting out or as supplementary channel. I mention this because as ONDC grows, an MSME might technically skip building their own site and just ensure their catalog is ONDC-listed so it shows up across apps (like Paytm, Meesho, etc.). It's a new model and we'll see how effective it is, but it's worth keeping an eye on.

When choosing, ask: - How quickly do I need to launch, and how much can I spend upfront vs. monthly? If you need to be live in a week and lack IT staff, go SaaS (Shopify, etc.). If you have more time and tight recurring budget, maybe invest in a WordPress site with WooCommerce and a one-time developer fee. - Do I need integrations with offline systems or unusual features? SaaS covers 90% of typical needs – product pages, cart, online payments, shipping labels, etc. If you have something unusual (say a build-your-own-product configurator, or user role-based pricing), check the SaaS app store if there's a plugin; if not, open-source might achieve it. - How do I plan to handle online payments and logistics? Most modern solutions integrate Indian payment gateways easily (Razorpay, CCAvenue, UPI, etc.). Ensure whichever you choose supports your needed payment methods (credit/debit cards, netbanking, UPI – nowadays they usually do). For logistics, many SaaS have partnerships (Shopify in India easily connects to Delhivery/FedEx via apps). With open-source, you may use services like Shiprocket which provide plugins to manage multi-courier shipping. Essentially, plan for how you'll get orders delivered – choose a tech that makes it straightforward to print labels, track shipments, and update customers (for example, some platforms can send automatic "your order is shipped, here's tracking" emails – a great customer experience point). - Scalability and performance: A slow site can kill sales. SaaS platforms are generally optimized for scale (their job is to keep your store fast globally). If your own site, choose good hosting. Initially, traffic will be moderate, but as an example, if you expect thousands of visitors during a sale, ensure your hosting plan can handle it or use cloud auto-scaling hosting. This may not be a concern until you grow, but keep it in mind (maybe avoid very cheap unknown hosts that might slow down with a slight traffic uptick).

One anecdote: a small fashion boutique started on a basic Wix store – very easy to set up, but as they added lots of high-res images, the site got a bit slow and SEO was limited. After a year, they migrated to Shopify which gave better speed and SEO control, and saw a boost in search rankings and conversions. The lesson is, it's okay to start simple and upgrade tech later as you learn what you need.

Mobile-first design is crucial whichever tech you pick. Most SaaS templates are responsive; if custom building, instruct developers to prioritize the mobile layout. Test the whole user journey on a phone (product browse, add to cart, payment). If something is fiddly (like a sign-up form with too many fields), streamline it.

Indian consumers are spoiled by the likes of Amazon's one-click order – they will drop off if your checkout is too cumbersome on mobile. Use features like social login or OTP login for ease if possible.

Also, think ahead about content management: you will need to update products, add offers, banners, etc. SaaS makes this easy through their admin panel. With open-source, ensure you or someone non-technical can handle routine updates via an admin interface.

In summary, choose a technology platform that fits your current resources and gives a bit of room to grow. It's often better to start with a solid template than to delay months trying to perfect a custom site. You can always refine as you get real feedback from online customers.

Now that tech and foundation are chosen, the next step is dealing with the nitty-gritty of payments, logistics, and compliance – essentially, fulfilling orders smoothly and legally.

Payments, Logistics, and Compliance

Selling online isn't just about the digital storefront; you must also collect payment, deliver the product or service, and abide by tax and legal rules. Let's break these down:

Payments

Indian online shoppers use a mix of UPI, wallets, cards, net banking, and COD (Cash on Delivery). To facilitate these: - Payment Gateway: If you have your own site, you'll integrate a payment gateway (like Razorpay, Paytm, CCAvenue, Instamojo, etc.). These providers aggregate various methods – UPI, cards, etc. Choose one with good success rates and easy setup. Many offer MSME-friendly pricing (often ~2% per transaction for credit cards, maybe lower negotiated for large volume, and some flat fee or annual fee plans). Check that it supports international payments too if you plan to sell abroad (some gateways have an option for accepting foreign cards, PayPal integration, etc.). Also ensure it can handle COD orders (usually COD is handled by logistics partner rather than gateway – see below). - Setup tip: Gateway onboarding requires KYC – have your business documents (GST, PAN, bank proof) ready. It can take 1-2 weeks to get fully activated, so do it early.

UPI and Wallets: UPI is huge (80% of retail digital payments). Most gateways now support UPI QR and intent. It's wise to allow UPI as a checkout option – it's frictionless especially on mobile (user just approves a collect request in their UPI app). - Cash on Delivery (COD): COD still forms a significant chunk of e-commerce orders (especially in certain product categories and non-metro areas). It builds trust – people may try your service COD first, then use prepaid later if happy. To enable COD on your own site, you typically allow the order to be placed without payment and mark it as COD. Your courier will handle collecting cash. Courier aggregators (like Shiprocket, NimbusPost, etc.) facilitate COD remittance to you (they collect from customer then deposit to your account after a certain time, often a weekly cycle). Note: COD has risks – higher returns (some people order and refuse delivery), and cash handling delays. You might consider offering small discount for prepaid to encourage it. But as a new online seller, offering COD will likely boost conversion by giving skeptical customers confidence to order. - Transaction Fees and Settlements: Understand the fee structure – e.g., 2% + ₹3 per transaction plus 18% GST on that fee. Factor this into pricing. Gateways usually settle amounts to your bank after T+2 or T+3 days (some offer faster settlement for a fee). COD settlements from courier can be 1-2 weeks. This affects your cash flow – plan accordingly (don't promise vendor payments expecting instant access to sale funds; there's a lag). - International Payments: If you plan to sell globally, set up ability to take USD/EUR etc. PayPal is one common option (especially for services or craft sellers, easy to add a PayPal button). Some Indian gateways allow multi-currency processing but check their rates (and RBI compliance – you'll need an Import-Export code and such for merchandise exports, we'll touch compliance soon). Keep in mind currency conversion costs and possibly slightly higher fraud risk with international cards (use 3D Secure where possible). - Security and Trust Seals: Use SSL (your site should show https:// and a padlock). Most SaaS platforms include this, or you can get free SSL via Let's Encrypt for your site. Having the padlock (no "Not secure" warning) is crucial – browsers and customers will flag you otherwise. Many payment gateways provide a "Secured by X" badge or you can display a PCI-DSS compliance badge if applicable – these small things reassure users that paying on your site is safe. Also, offer familiar payment options – e.g., showing "Paytm, PhonePe, Google Pay accepted" icons can comfort users who prefer those. - Smooth Checkout: Try to keep checkout steps minimal. Don't force account creation before order (you can offer guest checkout then ask to set password after ordering). The more fields and steps, the more drop-offs. Autofill and address lookup tools can help (pin code auto-fills city/state for instance). Also, clearly show total price including shipping and any taxes before final confirmation – surprises kill sales. If you can, integrate an address validation or serviceability check by pincode – either upfront (user enters pincode to see if you deliver there) or at checkout – to avoid taking orders you can't fulfill.

Logistics (Shipping and Delivery)

For physical goods, the e-commerce battle is won or lost on the last mile: - Choosing Couriers: You can tie up directly with major couriers (Blue Dart, Delhivery, etc.) but an easier route for MSMEs is to use a courier aggregator like Shiprocket, Pickrr, Vamaship, etc. They give you one dashboard to access multiple courier partners, compare rates by pincode, and schedule pickups. They often have no monthly fee – you pay per shipment (at discounted corporate rates because they pool many sellers). Early on, aggregators are a boon – you can ship across India without separate accounts and enjoy volume rates. As you scale, you might sign direct contracts with couriers for better rates or specialized services. - Packaging: Good packaging prevents damages and signals professionalism. Invest in proper materials – corrugated boxes, bubble wrap, tamper-proof plastic envelopes, etc., as needed. Brand your package if possible (even a sticker with logo) to build brand recall. But first ensure it's secure: products shouldn't rattle; use fillers. If shipping fragile items, label accordingly and check if courier covers damage (many won't unless you buy insurance). Note: for liquid/food, some couriers require extra sealing or disclaimers. Ask your logistics partner for any product-specific guidelines (e.g., batteries have special rules, liquids may need leak-proof packing). - Labels and Documentation: Your shipping tool or platform will generate an address label with barcode – attach that clearly. Also, include any required forms: e.g., for interstate commerce, a GST invoice must be inside or attached (some states also require an e-way bill if invoice value > ₹50k; but if you ship via courier under "courier waybill", often e-way not needed – verify current rules in your state). For international, you'll need customs declaration, export invoice, packing list, etc., and possibly importer's KYC. Initially, stick to domestic unless you research export process or use an assisted service. - Shipping Charges Strategy: Will you offer free shipping, flat rate, or charge actuals? Many sellers build an average shipping cost into product price and advertise "Free shipping" because customers prefer all-inclusive pricing. If your margins allow, this can increase conversion.

Alternatively, you can set a threshold like "Free delivery for orders above ₹500". If charging separately, be transparent up front (show in cart before checkout). Use weight-based or zone-based rate charts provided by your courier partners. A mistake to avoid: don't undercharge shipping significantly, or you'll bleed profit on faraway deliveries. Use shipping aggregator calculators to estimate typical costs to various zones and set your fees accordingly. - Delivery Time and Communication: Customers expect reasonably fast delivery (thanks to Prime). As a small seller, you may not match 1-2 day delivery nationwide, but do your best. Ship orders quickly – ideally same or next working day. Choose courier service types wisely (surface vs air) balancing cost and speed. Provide tracking numbers to customers as soon as shipped (most e-com platforms do this automatically by email/SMS if you input the tracking). Send updates – e.g., email/SMS like "Your order has been dispatched via X courier, tracking: …". Customers love being kept in loop. Also, clearly mention expected delivery times on your site (like "Delivery usually in 3-7 days depending on location"). It sets expectations and reduces "Where is my order?" queries. If using a shipping aggregator, some offer automated tracking notifications on your behalf – leverage that if possible. - Handle COD well: For COD, couriers will attempt delivery and collect cash. Ensure someone in your team monitors COD shipments and if they're undelivered (maybe buyer not home or changed mind), proactively reach out to customer or mark as return to avoid long hold in courier's network (returns cost you money). Also plan how you handle fake COD orders (some pranksters do this). You might confirm COD orders by call or OTP before shipping if that becomes an issue. Keep an eye on the ratio of returns from COD vs prepaid – you may refine strategy (like restrict COD for high-value custom items or far-flung areas if loss rate is high). - Returns and Customer Service: Not exactly shipping, but intimately tied. Have a process to handle returns: when a return comes back, inspect it quickly and process refund or replacement as per policy. Delays here frustrate customers immensely. Use your platform's features (if on marketplace, follow their return flow; if on your site, you might include a return form in the package or allow them to request via site). Keep records of returns so you can identify serial returners or problems with certain product batches. Also, if an item often gets returned due to damage, figure out if packaging needs improvement or if product description is misleading causing dissatisfaction. - International Shipping considerations: If/when you ship abroad, use an experienced international courier or aggregator. They'll guide on customs paperwork. Be aware of costs (international shipping can be very expensive relative to product price), so usually international sales make sense for high margin or unique products that foreigners can't get locally. Offer international shipping only if you've done the homework on pricing it properly and complying with export rules (IEC code, etc.).

There's also the option of selling via global marketplaces like Etsy or eBay – they have programs (Etsy will help with shipping or eBay's Global Shipping Program). But that's an expansion stage move.

Compliance (GST, Legal, etc.)

Doing e-commerce means a few extra compliance checkpoints: - GST and Taxes: If you are selling goods, you likely have GST registration (threshold ₹40 lakh for goods in most states, ₹20 lakh for services – lower if inter-state or on marketplace since they require it regardless of turnover). Online sales must be reflected in GST returns like any sales. Marketplaces will also deduct TCS (Tax Collected at Source) at 1% on the net value and deposit to your GST credit – you need to reconcile that. If you use your own site, no TCS scenario. Ensure you apply correct GST rates on products. Most e-com platforms allow you to set the tax rate per product. If you sell exempt goods or have composition scheme, check rules (composition dealers cannot sell through marketplace as per GST law). Keep invoices for all shipments – many couriers won't pick up without an invoice copy for commercial shipments. - Import/Export: For international sales (even via marketplaces that ship abroad), you need an IEC (Importer Exporter Code) from DGFT (simple online process). Also, you must file periodic export data in GST returns (exports are zero-rated but you either do LUT or claim refund of GST if paid). If you're not ready for this paperwork, consider sticking to domestic until you can engage a CHA (customs agent) or learn processes. An alternative is using cross-border platforms like Etsy which simplify a lot but you still need IEC as the exporter of record in many cases. - Legal Metrology & Consumer laws: If you sell packaged goods, you must comply with labeling laws (Legal Metrology Packaged Commodity Rules) – which require certain declarations (net weight, MRP, customer care, etc.) on the product. Also, e-commerce rules require that your product listing shows specific information: e.g., MRP (with all taxes), origin (Made in India or imported), manufacturer name & address, common generic name of product, etc. Marketplaces enforce this for you by requiring those fields when listing. On your own site, make sure to include such info on product pages to be compliant. - Data Protection: You'll have customer personal data (names, addresses, phone, possibly emails). Keep it secure (don't share it, protect it from breaches).

India's new data protection bill will likely mandate explicit consent and reasonable security practices even for SMEs. Basic compliance would be having a privacy policy on your site, using data only for fulfilment and not spamming customers without opt-in, and honoring any customer request to delete data if they ask (especially from EU citizens if you sell internationally, due to GDPR). These laws are evolving; stay updated. - Intellectual Property: Ensure you're not accidentally infringing someone's IP (like selling unlicensed fan-merch etc. can get you delisted or sued). Also protect your own IP – if you have trademarked your brand or designs, list that on marketplaces (they often have programs like Amazon Brand Registry to safeguard your listings from copycats). Avoid using images or text in your content that you just grabbed from Google – use your own or properly licensed ones, to avoid future copyright issues. - Local Laws and Sectoral Rules: If you deal in specialty items (food, cosmetics, medicines, etc.), there are additional laws. FSSAI for food – you need a license and must display FSSAI number on listings of food products online as well (some marketplaces have a field for it). For ayurvedic medicines or cosmetics, make sure you comply with labeling and don't make claims not allowed. If selling electronics that need BIS certification, have it in place or you risk packages being stopped by authorities. Essentially, the regulations that apply to selling offline still apply online, plus some specific e-com ones.

This can sound heavy, but if you are already a compliant business offline, most is common sense extension to online. Many MSMEs go online informally at first; while that might slip under radar for a bit, as you scale it's vital to get formal – register that GST, file those returns, etc. Not only to avoid penalties, but many consumers and businesses only want to deal with compliant vendors (e.g., you need GST to sell on GeM or to bigger companies who take input credit). It also gives you advantages like being able to open current accounts, get loans, etc., which you'll need as you grow.

At this point, we have covered setting up shop and fulfilling orders. The next big aspect is getting people to find your online store and persuading them to buy – i.e., marketing and driving traffic, then analyzing data to optimize. Let's explore those.

Driving Traffic and Sales

"Build it and they will come" does not hold true in e-commerce. Once your online store is up, you need to actively bring in potential customers. There are two broad avenues: organic (unpaid) and paid channels.

Organic Channels

These methods don't cost (much) money, but rather time and creativity: - Search Engine Optimization (SEO): This means optimizing your site so that when people search relevant keywords on Google (or Bing, etc.), your site ranks high in results. For example, if you sell khadi shirts, you want to appear when someone searches "handwoven khadi shirt India" or "best khadi clothing online". Key steps: - Research keywords that potential buyers use (Google Keyword Planner or even just observe autocomplete suggestions). - Use those keywords naturally in your page titles, product descriptions, meta tags. E.g., title might be "Handwoven Khadi Cotton Shirt – Men's Kurta (Natural Dye) – YourBrand" which hits various likely search terms. - Ensure your site is crawlable (SaaS platforms do this for you; if WordPress, use an SEO plugin like Yoast to set meta descriptions, etc.). - Get other sites to link to you if possible (maybe a local blog reviews your product, or you write a guest article somewhere). Such backlinks improve SEO.

SEO is a long game but critical. The aim is to have a steady stream of "free" visitors who found you on Google. For local businesses, also optimize Google My Business listing (so you show up in Google Maps for relevant local searches).

- **Content Marketing:** This involves creating content (blogs, videos, infographics) that draws people in. For example, a company selling accounting software might write blog posts like "5 GST Filing Tips for Small Businesses" which attract MSME owners via search and establish credibility (some will then check out their software). Or a baking supplies store might post recipes and cake decorating video tutorials – people come for the content, and the content gently promotes their products ("To do this, we used XYZ baking mold available on our site"). Consider what knowledge you have that potential customers would value. It also gives you material to share on social media or via email newsletters.

- While not immediate sales, it warms up an audience and builds trust (and helps SEO too).
- **Social Media (Organic):** We touched on using social commerce to sell, but even if you don't sell directly on social platforms, you should likely have a presence there. Identify which platforms your target customers use – Instagram for younger lifestyle/fashion, LinkedIn for B2B/professional services, Facebook for general consumer reach, maybe YouTube for how-to content across all domains. Then consistently share engaging content: product photos in real use, behind-the-scenes videos, customer testimonials, tips related to your niche, etc. The goal is to build a follower base who might convert to customers or who amplify your message. Respond to comments and messages promptly – social media is a two-way street. Success here doesn't necessarily mean millions of followers (which might not translate to sales). Even a few thousand engaged followers can drive steady traffic and word-of-mouth. Use relevant hashtags (e.g., #MadeInIndia #organicfood) to appear in topic searches. Also, join relevant groups or communities – e.g., if you sell industrial tools, participating helpfully in engineering forums can indirectly draw people to your site.
- **WhatsApp and Email Marketing (to existing contacts):** Leverage your network. WhatsApp Business allows broadcast lists (so you can send new product announcements to many at once without starting a noisy group chat). Just avoid spamming – make sure recipients either gave consent or are likely interested (e.g., past customers or business contacts who agreed to updates). Same with email – start collecting email addresses (from site sign-ups, from order history, or events you attend). Then periodically send a newsletter: highlight new arrivals, a limited-time sale, or share a useful tip related to your products. Keep emails short, visually appealing, and mobile-friendly. Services like MailChimp (free up to a certain number of subscribers) help manage email campaigns and ensure compliance (unsubscribe links, etc.). These direct channels are great for driving repeat sales: e.g., a person bought once, an email about "New stock for the festive season" might make them buy again.

- **Online Marketplaces (Organic presence):** If you are on a marketplace like Amazon, it's not exactly "organic" because you're on their platform, but some techniques are akin to SEO: optimize your product title and description with keywords buyers search on that marketplace. Encourage satisfied buyers to leave reviews (perhaps via a follow-up thank you email through the marketplace system). Answer customer questions on the listing openly – these Q&As also become part of the page content and help future shoppers. Essentially, if marketplace is a channel, treat your listing as a mini-site to be optimized – good content, good images, and good service that leads to positive ratings. That organically boosts your ranking within the marketplace (Amazon's algorithm heavily factors conversion rate and ratings).
- **Referral Program:** Encourage existing customers to refer others by providing a small incentive – e.g., "Refer a friend and you both get ₹100 off." This can be tracked via unique referral codes or simpler, just ask new customers to mention who referred them (then you send a coupon to the referrer). Word-of-mouth is extremely potent for SMEs; a formalized referral offer can stimulate it. There are referral plugins or you can manage it manually for a start (issue bespoke coupon codes to your top 10 customers to share with friends, etc.).

The beauty of organic channels is they build sustainable advantage – a high Google ranking or a loyal Instagram following continues to pay dividends without proportional spend. But it takes time to build. That's where paid channels can complement by giving you a boost, especially in the early days or around key campaigns:

Paid Channels

Money can buy you visibility. Key paid methods include: - Search Engine Ads (SEM): Google Ads (and Bing Ads to a lesser extent) allow you to show your site at the top of search results for certain keywords, marked as "Ad." For example, you can bid to show your ad when someone searches "buy organic honey online." You pay a cost-per-click (CPC) when someone clicks your ad. This can range widely – ₹2 to ₹50 or more per click depending on competition for that keyword (insurance, for instance, is expensive; niche handicrafts might be cheap). Google Ads also offers Shopping ads where product images with price show up (requires uploading a product feed to Google Merchant Center). Pros: Immediate visibility on relevant queries, can be turned on/off or scaled quickly. Cons: Costs can add up; not all clicks lead to sales (so you have to monitor and optimize or you might overspend on broad keywords that don't convert). But it's a great way to attract customers actively searching for what you offer, especially while your SEO is still building. Tip: start with specific (long-tail) keywords that indicate high intent (e.g., "organic ajwain honey 1kg price" – someone searching that is likely ready to buy if they find a good offer).

Also, set a moderate daily budget initially (say ₹500/day) and see how it performs. - Social Media Ads: Platforms like Facebook/Instagram, LinkedIn, Twitter, etc., offer targeted advertising. You can target by demographics, interests, behaviors, locations, etc. For instance, an ethnic apparel brand could target women aged 22-45 in metro cities who have shown interest in ethnic wear or follow related pages. These ads can be powerful for creating awareness or retargeting (showing ads to people who visited your site but didn't buy). Pros: Visual format helps showcase product; targeting can be very granular; costs per impression or click can be relatively low (especially on Facebook/Instagram where ₹1000 might reach tens of thousands of eyeballs, depending on targeting). Cons: It's interruptive marketing – people on social media aren't actively looking to buy right at that moment, so conversion rates are usually lower than search ads. The creative matters a lot – you need an eye-catching image/video and concise message to stop the scroll. For LinkedIn (if you do B2B marketing), costs are higher but targeting professional attributes is unique (e.g., show an ad only to supply chain managers in pharma companies if you sell lab equipment – very possible on LinkedIn). - Marketplace Promotions: If you sell on a marketplace, they each have their internal ad system (Amazon Sponsored Products, Flipkart Product Ads, etc.). Using these can bump you to page 1 for keywords on that platform. Particularly useful in crowded categories or for new products with no sales history. For instance, you could advertise your new smartphone accessory for the keyword "Bluetooth earphones" on Amazon – you'll pay a CPC for clicks. Pros: Speeds up initial momentum; once a product gets some sales and reviews, you can taper down ads and let organic take over. Cons: It's easy to burn money if you don't monitor – some sellers overspend chasing rank and lose margin. Start with a small daily budget and target specific terms related to your product rather than broad category terms (which might be dominated by big brands and get lots of clicks but low conversion for you). Over time, optimize: turn off ads on keywords that don't convert for you. - Retargeting Ads: These are ads shown to people who have interacted with you before – like visited your site but not purchased, or added to cart but not completed order. You've likely seen these yourself ("that pair of shoes follows you around the internet after you looked at it once"). Retargeting is effective because the audience is warm – they know your brand already to some extent. You can do this via Google Display Network or Facebook Ads (install their pixel on your site which builds a custom audience of site visitors, then run ads to them). Pros: Often higher ROI since these folks showed interest. Good for converting "window shoppers" into buyers by reminding them or offering a slightly sweeter deal ("Still interested? Use code SAVE10 for 10% off"). Cons: Need enough initial site traffic to have an audience to retarget; also frequency should be controlled (don't stalk users for months – set ad frequency caps and a duration, e.g., only retarget up to 2 weeks after their visit, else it gets annoying). - Influencer or Sponsored Content: This is paying individuals or publishers to promote you – e.g., an Instagram fashion influencer posts wearing your dress and tags your handle (you might gift the item or pay a fee), or a YouTuber reviews your gadget. In B2B, it could be sponsoring an industry newsletter or webinar. Pros: Leverages trust and follower base of the influencer – can yield sales if authentic and target fits (micro-influencers with 10k loyal followers often drive more action than a generic celebrity shoutout). Cons: Results can be hit-or-miss and hard to track (use unique coupon codes or trackable links to see what comes from that campaign). Also, finding the right influencer (with genuine engagement and whose audience matches yours) is key; otherwise you pay and get little. Always disclose proper if needed (ethical and in some jurisdictions required to mark as ad). Start small: maybe collaborate with a couple of micro-influencers for product-for-post deals to test waters before considering bigger paid collaborations.

No matter which paid channels you try, track the metrics. Use UTM parameters on URLs and check Google Analytics to see which campaigns are driving traffic and conversion. Calculate rough Customer Acquisition Cost (CAC) from each channel (total spend on channel / number of customers acquired from it). Compare with the Lifetime Value (LTV) of those customers (if you have repeat purchase business). As a simple rule: CAC should be less than the profit from the first order ideally, or at least justified by LTV if you know customers will buy again. For instance, if you spend ₹500 in ads to get one customer who orders ₹1000 of goods at 30% margin, you actually made only ₹300 gross profit, which doesn't cover the ₹500 ad spend – that channel is unprofitable unless that customer is likely to order multiple times in future. This analysis helps decide where to scale up and where to cut spend.

Often, businesses use paid channels to kickstart – e.g., first 6 months heavy on ads to build customer base, then relying more on repeat business and organics. It's a balance: too little spend and no one finds you, too much and you might get growth but with losses. So start modest, experiment (A/B test ad creatives and audiences), and optimize constantly.

Analytics: Measuring and Improving

A big advantage of online business is the wealth of data you can get. But data is only useful if you act on it: - Set up Analytics Tools: Install Google Analytics (GA) on your site – it's free and shows how many people visit, from where, what pages they see, etc. For marketplaces, use any dashboards they give (Amazon has business reports on sessions, conversion, etc.). If selling through social media, look at profile insights (Instagram offers reach, engagement stats for business accounts). These help gauge overall performance. - Track Key Metrics: Common e-commerce KPIs: - Traffic/Visitors: How many people visit your site (or see your products on marketplaces). - Conversion Rate: The percentage of visitors who make a purchase. E.g., if 100 people visit and 2 buy, conversion = 2%. A typical small e-com site might see 1-3% initially. If yours is much lower, investigate why (is site slow, product not compelling, etc.). Marketplaces often have higher conversion because people there are ready to buy. - Average Order Value (AOV): Total revenue / number of orders. If you can increase AOV (like by cross-selling or bundling), you earn more per customer, which can offset ad costs. - Bounce Rate: % of visitors who leave immediately without interacting. If bounce is high (>70%) on your site, that could mean wrong traffic (people coming expecting something else) or a poor landing page (maybe it loads slow on mobile or is visually unappealing). Optimize content or targeting to reduce bounce. - Cart Abandonment Rate: Many add to cart but don't complete checkout – track that. If it's, say, 60% (which is common in retail), try to improve by sending reminder emails ("You left something in your cart"), simplifying checkout, or offering a small discount for completing the order. There are tools to automate an email within a few hours of abandonment if user provided email in cart. - Customer Acquisition Cost (CAC): As discussed, know roughly what you're spending to get a new customer. Break it by channel if possible. This lets you allocate budget smarter. - Repeat Customer Rate: How many of your orders each month are from previous customers vs new. If you see a healthy repeat rate building (e.g., 20-30% of orders from returning customers by month 6), that's great – it means your product and service satisfy, and you should nurture that base (via loyalty programs, new product announcements).

Geographical data: See which cities or regions most customers come from. You might focus ads more there or even plan distribution accordingly (e.g., stock inventory at a warehouse in that zone for speed). For example, an MSME saw most of his organic food orders came from Bengaluru and Mumbai – so he did city-specific Facebook campaigns there which performed well (since interest was proven), rather than broad national targeting. - Product Performance: Identify which items are top sellers and which hardly move. Push the winners (maybe consider expanding their variants, or highlighting them on home page). For the slow movers, figure out why – is it lack of visibility (maybe burying in site navigation) or truly low demand? Maybe discontinue or replace those to avoid tying up capital.

- **Use Analytics Insights:** Don't collect dust. Set a routine – maybe every Monday review the past week's data. Look for anomalies: did a certain blog post bring a spike of traffic? Did conversion drop after a site redesign? Did a particular ad campaign show a high bounce rate, meaning its landing page might be irrelevant? The numbers often tell a story: e.g., if mobile conversion is half of desktop conversion, maybe your mobile site needs improvement.
- **Test and Iterate:** Use A/B testing for elements on site – e.g., try two different homepage banners and see which yields more clicks or sales (there are tools like Google Optimize for simple tests). Or test two versions of ad copy to see which gets better ROI. E-commerce is continuous improvement – even giants constantly tweak page layout, button colors, etc., to see what lifts sales. For an MSME, start with bigger wins (like improving product descriptions across site could raise conversion more than fiddling with button color). But over time, these optimizations stack up.
- **Customer Feedback Loop:** Analytics give quantitative data, but also seek qualitative input. Encourage buyers to leave product reviews or do a post-purchase survey ("How did you find us? Was the ordering process easy? Any suggestions?"). This feedback can highlight issues or ideas not obvious from numbers. For instance, reviews might mention "runs small, order one size up" – if you see that, update your description to guide future buyers and reduce returns.
- **Keep an Eye on Competitors:** Use tools or manual checks to see how others are doing. For example, search your target keywords on Google periodically – see who else appears (maybe they have a blog post ranking above you – can you write a better one?). On marketplaces, look at competitor pricing and reviews to position yourself. There are even tools to track competitors' online promotions, stock status, etc., though as an MSME you may not need that depth.

- Just being aware – e.g., if a competitor launched a new feature or got media coverage leading to an online traffic jump – can inform your strategy ("They got a lot of traction by offering a subscription plan… maybe we should consider subscription model for our consumable product").

The data-oriented approach keeps you agile. For example, one MSME dealing in home decor saw via analytics that Pinterest was an unexpected traffic source – people pinned their product images and that drove visits. Noticing this, they started actively posting on Pinterest and optimizing images for that platform (taller aspect ratio, adding decorative text on image) and saw even more referral traffic and sales from it.

In summary, treat data as your friend – it points out where you're losing potential customers (e.g., heavy drop-off at checkout step 2 = maybe step 2 asks for too much info or is broken on mobile), and where you can double-down (e.g., a certain product has great conversion rate = it's a hit, so promote it more).

Bringing it all together: By setting a strong foundation (good products, content, easy tech), driving traffic through multiple channels (marketplaces, SEO, social, ads) and then measuring and refining based on real data, you create a growth engine. Initially, it might feel like a lot of moving parts, but you can start small (maybe start on one marketplace + one social platform + a basic site), then add and refine as you gain confidence.

Finally, let's consider scaling up beyond the initial expansion – thinking 6-12 months ahead, how to evolve your e-commerce presence from a side channel to a core part of your business strategy.

Industry-Specific Examples (short, practical)

(To ensure we cover a breadth of scenarios, let's touch on a few industry-specific e-commerce tactics, as requested in the outline):

- **Manufacturing (B2B focus):** A small component manufacturer might not sell to end consumers, but establishing an online catalog and inquiry system can streamline dealings with PSU or MNC buyers. For example, listing products on IndiaMart or your own site with detailed specs and an "Add to RFQ" cart can speed up the quotation process.
- Some manufacturers use e-commerce just for small spare parts or replacement orders, while bulk orders still go via offline contracts – that's fine; the online channel can complement by handling the low-volume, long-tail sales efficiently. Also, consider participating in the government's GeM portal as an e-supplier – MSMEs have an edge there due to preference policies, and it's essentially e-commerce to government departments.
- **Services:** While selling services online is a bit different, many principles apply. If you're an HR consultancy, set up a site where clients can purchase fixed-price service packages (e.g., "Resume review – ₹1000" or "Virtual 1-hour legal consultation – ₹5000"). They pay online, you deliver service via Zoom or email. This productization of services allows even a one-person consultancy to "sell online." You'd focus on content marketing (blogs, LinkedIn thought leadership) to drive traffic, and leverage scheduling and delivery tools (maybe integrate Calendly for appointment booking with payment). Social proof like client testimonials are crucial here because trust is key.
- **MSMEs in Retail/Distribution:** If you're a distributor who traditionally supplies shops, you could consider going D2C online to get better margins (many Indian SMEs are doing this – e.g., a regional snacks distributor launching a direct online store and Flipkart listing to reach consumers nationally). It can coexist with your B2B business. Just ensure you manage channel conflict (maybe keep pricing consistent or offer different SKUs for D2C). The flip side: if you're a retailer (a physical shop), getting on e-commerce can greatly expand your catchment – many local stores became "dark stores" fulfilling online orders during lockdowns and continued because it added sales. Tie up with hyperlocal delivery (Dunzo, Swiggy Genie) for local quick delivery, and use courier for farther orders.
- **Export-Oriented MSMEs:** If you make handicrafts, textiles, etc. for export, consider global marketplaces like Etsy, Amazon Global, eBay. They connect you to international buyers without you having to market from scratch in those countries. Many Indian handicraft sellers find success on Etsy due to high demand for authentic products. There are logistics programs (like Etsy's India Post tie-up) to help ship abroad. The key is to follow platform guidelines (e.g., for Etsy, it's about storytelling and authenticity). Over time, you could even launch your own international storefront if volume merits, but starting on a known platform is wise.
- **Edible Products:** If you sell food items, e-commerce opens a huge geographic market, but pay attention to shelf-life and shipping conditions (chocolates may melt, etc.). Start by targeting zones where delivery can be done within the product's freshness window. Use proper packaging (insulated boxes, etc., if needed).

- Build trust with FSSAI license display and by encouraging reviews (because new buyers are wary about food quality online). Many small food businesses do well via Instagram and WhatsApp communities (like home bakers or regional snack sellers), which then evolve into full-fledged online brands listed on marketplaces or their own sites. The advantage in food is strong repeat if people love the taste, so focus on retention (subscribe & save options, loyalty discounts for frequent buyers, etc.).

As you can see, strategies may tweak slightly by sector (services focus more on content, exports more on specialized marketplaces, etc.), but the core approach remains: get online visibility, provide an easy purchase process, and deliver as promised to build trust and repeat business.

Tool Landscape: From No-Code to Enterprise

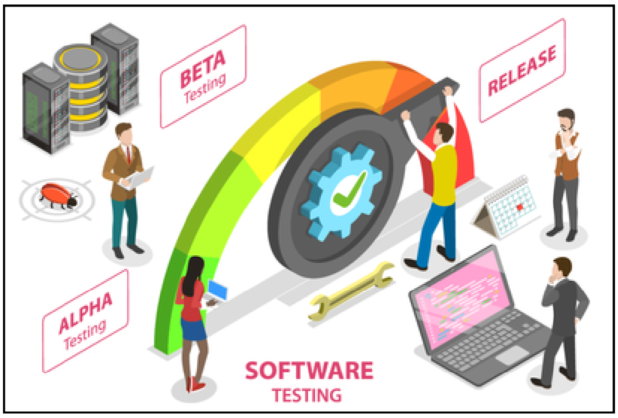
(The outline suggests a section here, but we've largely covered tech platforms earlier. Possibly we can mention low-code integrations or scaling tools in brief, but to avoid redundancy, I'll treat this as partially covered in the "Choosing Technology" section. I will ensure we mention no-code vs enterprise and integration – we did talk about that. We can highlight criteria to select tools like we did. So I'll consider this sufficiently covered above.)

(Moving on to governance, but that was more relevant to cloud – likely the "Data, Privacy, Governance" section we did for e-commerce suffices for that outline point. Up next is combining everything into a roadmap, which we'll interpret as the 6–12 month plan, already requested.)

6–12 Month Roadmap for a New E-commerce Business

Establishing and growing your e-commerce presence is a journey. Let's outline a pragmatic phase-by-phase roadmap for roughly the first year of going online:

- **Quarter 1 (Months 1–3): Lay the Groundwork and Launch**
- **Finalize Product and Pricing for Online:** Decide which products/services to start selling online. Ensure you have attractive pricing (account for platform fees/shipping in your pricing). If needed, create e-commerce specific bundles or smaller packs that are easier to ship.
- **Set Up Online Channel(s):** Choose your primary channel and get it running. For instance, build your website using a platform like Shopify or set up your Amazon/Flipkart seller account and list products (you can do both concurrently if bandwidth allows). Ensure all the foundation elements we discussed (content, images, policies) are in place.



- **Complete Necessary Registrations:** Register for GST if not already (most platforms require it). Get your FSSAI if selling food, IEC if planning to export, etc. Also, register your brand trademark if you foresee brand-building (it takes time, so earlier the better; meanwhile use TM symbol).
- **Beta Test and Soft Launch:** Before shouting from the rooftops, do a trial run. Place a couple of test orders (maybe have friends or family across different locations order through your site or marketplace listing). This will test payments, packaging, courier pickup, delivery times, and your internal process (printing invoice, updating stock). Work out any kinks (e.g., if shipping takes longer than expected, adjust messaging; if a payment method had an issue, fix it).
- **Official Launch Promotion:** Announce your online store through whatever channels you have – email your existing customer list, post on social media, perhaps a small ad campaign targeting your city or niche. Maybe offer a "Launch Week" promo code to encourage first orders. The goal in Q1 is to drive those initial sales and gather feedback. Don't be disheartened if slow at first – each order is a chance to learn and get a review.
- **Customer Service System:** As orders come in, set up a simple tracking method for customer inquiries (even if it's just an Excel or using a helpdesk software's free tier). Respond quickly to questions or issues – as a new seller, responsive support can turn a curious visitor into a loyal customer.
- **Quarter 2 (Months 4–6): Drive Traffic and Optimize Conversion**
- **Scale Marketing Efforts:** Based on what worked in Q1, ramp it up. If Google Ads brought good traffic, increase budget modestly.

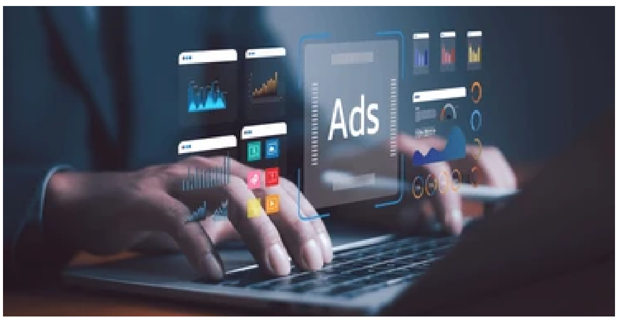
- If social media content got engagement, post more frequently or consider a small collaboration (e.g., an influencer campaign). Continue SEO work – perhaps write 2-3 blog posts addressing common search queries related to your products.
- **Introduce Additional Sales Channels:** If you launched with your own site, now consider also listing on a marketplace (or vice versa). More channels = more reach. Ensure you have bandwidth to manage them (maybe use a tool like Browntape or Unicommerce to centralize inventory across channels if manual updating gets tough).
- **Analyze Data & Improve Site:** By now you have some site analytics and user behavior data. Identify bottlenecks – e.g., if many users drop off at shipping page, maybe your shipping charges are too high or unclear. If a product gets lots of views but few buys, consider why (maybe price too high or description not convincing; check if competitors selling same item cheaper). Make improvements accordingly – tweak prices, adjust page layouts, add an FAQ section to product pages to address common doubts.
- **Build Trust Signals:** By Q2, hopefully you have some happy customers. Solicit reviews/testimonials and display them. If you can gather user-generated content (like a customer photo with your product), feature it (with permission) on social or site – it builds authenticity. You can also add trust badges on site ("100% Secure Payments", "Free Returns within 7 days", etc., whatever applies).
- **Expand Product Range or Stock:** If certain items sold out quickly or you got requests for variations (maybe people ask "Do you have this in red?"), consider expanding the catalog to cater to demand. Ensure you manage stock levels to avoid stockouts – if you see one item trending, produce/procure more ahead of time. Conversely, if some products didn't sell at all, you might phase them out or try a clearance discount to move inventory.
- **Customer Engagement and Retention:** Start a regular pattern of engaging existing customers to drive repeat orders. For example, send a thank-you coupon code after their first purchase (valid for next 3 months). Launch a simple loyalty program (even if just "buy 5 times, get 6th free" tracked manually).
- This quarter, focus not just on new customers but keeping previous ones in the loop via emails or WhatsApp updates (without spamming).
- **Quarter 3 (Months 7–9): Scale Operations and Explore Growth Opportunities**
- **Streamline Operations:** If order volume has grown, invest in tools or processes to keep service quality up. Maybe start using an order management system if you haven't, or hire a part-time packer or customer support assistant. Ensure your return handling is efficient now that you have more transactions (set up a dedicated day or person each week to process returns/refunds so nothing falls through cracks).
- **Improve Site Features:** Based on feedback and competition benchmarking, add site features that can boost sales. For instance, enable a "Related Products" carousel to upsell, integrate a live chat plugin for instant query resolution (could simply be WhatsApp chat link if full chat software is overkill). If many customers ask similar questions, add those as a Q&A on the site for self-service.
- **Explore New Markets:** By now you have a hang of domestic shipping. Consider if you want to start serving international orders (if relevant and profitable). If yes, this quarter obtain the export paperwork (IEC) and list your products on a global platform or your site with international shipping enabled. Alternatively, if you're mainly in one region of India, consider focusing marketing to new states where you got a few orders organically – push more there to grow national footprint.
- **Festive/Campaign Preparation:** Many businesses get a large chunk of sales during festive seasons or yearly sales. Identify which ones matter for you (Diwali, Christmas, wedding season, financial year-end for B2B, etc.). Start planning a special campaign or offers for that – decide products to highlight, procure extra inventory if needed, design ads/banners in advance. Q3 might include one big season (e.g., Dussehra/Diwali). Make sure you're ready with stock and marketing to ride that wave – often MSMEs see their site traffic double during such times if marketed right.
- **Monitor Financials:** As you scale, ensure to check that increased sales are also increasing profit, not just top-line. Re-calc your effective margins after accounting for all e-com costs (packing materials, shipping fees, gateway fees, returns losses). Identify where you can cut cost or increase price slightly to maintain profitability. For example, maybe you realize courier costs are eating too much; you could negotiate with your aggregator for a better slab rate now that your volume is higher, or decide to introduce a shipping fee above a certain weight rather than free shipping for all orders.

- Customer Feedback Loop: By month 9, consider doing a survey among your repeat customers – ask what they like and what could be improved. Could even incentivize it (chance to win a ₹500 voucher for completing survey). This direct feedback can reveal opportunities for new products or needed service improvements that internal data might not show.

- **Quarter 4 (Months 10–12): Consolidate and Expand Reach**
- **Evaluate Channel Performance:** Look at a full year view. Which channel gave most sales? Highest ROI? Worst return rate? Use that to plan the next year. Maybe you find marketplace sales outpaced your own site 3x – then next year allocate more inventory and ad budget to marketplace where it's working, but also question why site lagged (was marketing insufficient or site conversion poor?). Conversely, if your own site built a loyal base and marketplace was more hassle than it's worth (happens in niches where community matters), you might reduce marketplace focus.
- **Scale Advertising for Peak Season:** If say December or Jan is big for you, in Q4 go aggressive (assuming you've fine-tuned your ads by now to be cost-effective). This could be the time to do an ad blitz or a social media contest to amplify brand presence now that fulfillment and site are running smoothly.
- **Consider Advanced E-com Techniques:** If you've grown enough, you can implement more sophisticated strategies: for example, a subscription model (get products auto-delivered monthly – secure recurring revenue), or selling in new channels like ONDC (the open network – by end of year, see if joining ONDC seller side can open an additional sales avenue as it gains traction). Perhaps launch a mobile app if you have many repeat customers (apps make reordering easier, though getting people to install is a challenge – weigh the benefit).
- **Team and Infrastructure:** By one year, gauge if you need to build a team. Perhaps hire a dedicated e-commerce manager or a digital marketing person if you as owner have been juggling it all. Also consider warehousing needs – is your home/office overflowing with inventory now? You might rent a small warehouse or use a 3PL fulfillment service for storage and dispatch if volume is large. This is the time to ensure your operations can sustain the growth pace without compromising service quality.
- **Governance and Compliance Check:** With growth, ensure you haven't let compliance slip. Do an internal audit of all GST filings, marketplace TCS credits, etc., to make sure accounts reconcile. If you had made any ad-hoc arrangements in the rush (like shipping some items without proper invoices early on), get everything formalized and clean. Being a year in business, you may face more scrutiny (e.g., GST department might flag differences between marketplace TCS and your return; or MCA might require additional reporting if you're a company). So make sure back-office is solid.
- **Plan Year 2 Strategy:** Lastly, use this quarter to strategize beyond immediate. Identify new product lines to add based on demand trends, new marketing channels to experiment (maybe try content on a new platform like starting a YouTube channel since you now have more resources for it), and set targets for Year 2 (e.g., double sales, expand internationally, or improve profit margins by X%). A clear plan helps align any investments needed (maybe you'll invest in better packaging equipment or in-house content studio, etc., to support that plan).

This roadmap is generalized, but it gives a structure: start small and lean, focus on getting things right for a few months, then gradually ramp up marketing and offerings, continuously refine by data, and by end of year be in a position to either scale faster or maintain a strong, efficiently-run online business as a core part of your revenue.

Throughout this journey, stay customer-centric – as you grow online, you'll gather a community of buyers; nurture them through great service, engagement, and by adapting to their needs. Happy online customers become brand ambassadors, leaving good reviews and referring others – the cheapest and best marketing you can get.



Conclusion: E-commerce as a Growth Engine, Not Just a Sales Channel

E-commerce isn't just an additional sales channel; done right, it can become a growth engine that transforms your business. By establishing a digital storefront, you break past geographical limitations – a boutique in Kanpur can find customers in Kochi; a tool manufacturer in Ludhiana can receive orders from NTPC plants across the country. Online presence also means better data and customer insight – you learn which products are hits, what customers search for, and can quickly adapt to market signals (something traditional channels relay much slower).

Having an e-commerce capability also strengthens your position with large buyers. PSUs, MNC procurement teams, and government bodies increasingly use digital methods to discover and evaluate vendors. An MSME that is e-commerce savvy (with a professional website, active marketplace ratings, etc.) signals that it is modern, responsive, and able to integrate with digital supply chains. In vendor selection, this can tip the scales in your favor over a competitor who's stuck in all-offline ways. Some large companies even prefer ordering via vendors' online portals or through B2B networks as it's more efficient – if you can offer that, you become a more attractive partner. In essence, your digital readiness becomes a competitive advantage in B2B as well, not just in retail.

A key point to remember: e-commerce is not a zero-sum against your existing channels. It can complement retail distributors, augment exports, and provide resilience (as seen during COVID-19 when businesses with online routes survived better). It also allows you to build a direct relationship with end customers even if you mostly sell via intermediaries – for example, a small appliance brand might mostly sell via dealers, but also run an online store where they can hear feedback directly, offer accessories, and reinforce brand loyalty with content and service. This direct connect is invaluable in a world where understanding consumer preferences quickly is gold.

Finally, the barrier to entry in e-commerce has lowered significantly: with no-code tools, one can go online in days, and marketplace on-boarding for MSMEs has been simplified by initiatives and support from companies and government (e.g., Amazon and Flipkart have MSME seller support programs; GoI has training for small artisans to sell online). If you haven't started yet, the best time is now – start with one product on one platform and learn as you go. If you're already selling online, there are always new strategies or markets to try – e-commerce is dynamic, so keep experimenting (maybe ONDC or social commerce or a new international market).

To wrap up, here are a few action-oriented closing thoughts: - Just Start: If you've been on the fence, take the first step – list one product on a marketplace or set up a basic site this quarter. The insights from actually operating will teach more than months of planning. - Learn and Iterate: Use the rich data e-commerce provides to make smart decisions – treat each low sale item as a lesson (either improve it or drop it), each marketing campaign as a test (double down if ROI positive, tweak or stop if not). - Stay Customer-focused: What wins online is understanding what customers want and delivering it conveniently. Keep gathering feedback, watch reviews, reply to comments – show that you care more than faceless big companies. That human touch can be your differentiator. - Step by Step: You don't need to launch with 100 products and an omni-channel presence from day one. Expand gradually – it's better to provide excellent service on a smaller scale and build a good reputation, then scale up, rather than overextend and get bad reviews due to lapses.

E-commerce isn't a sprint, it's a marathon that can steadily accelerate your growth trajectory. With the strategies and points we discussed – from solid foundations to savvy marketing and continuous analysis – you can turn your online storefront into a significant revenue driver. More importantly, you'll future-proof your business in a world where digital commerce is not just for a few but for everyone from consumers in small towns to large organizations doing procurement.

The digital marketplace is vast and growing – start small, think big, and build step by step. The opportunities are enormous, and with a thoughtful, human approach (blending technology with good old customer service values), your MSME can not just participate in but truly leverage e-commerce as the engine of growth, profitability, and competitive strength in the years to come.

CMA Shradha Singh

CMA Shradha Singh is a qualified Cost and Management Accountant who secured an All India Rank in the CMA Final Examination, a distinction that reflects her dedication, discipline, and strong command of finance, costing, and business strategy. She also holds a postgraduate degree in Commerce from Dr. Ram Manohar Lohia Avadh University (RMLAU).
Editorial Board Member, The Worldonomics Times

Section 54EC Bonds: A Way to Save Tax on Capital Gains

As we all know that selling property in India at a great profit attracts the huge amount of tax burden. This is the common scenario in India but there is a way to save huge chunk of taxes by just simple investment in "Long Term Specified Bonds" or "54EC Bonds". **Section 54EC Bonds (Section 85 as per The Income Tax Act, 2025)** offers the great opportunity for the investors to reinvest their long term capital gains in such specified bonds to enjoy maximum tax exemptions with minimum risk. But it is crucial to understand that the gains from shares, mutual funds or any other securities are ineligible for reinvestment under 54EC Bonds. The gains from selling land and building are only eligible for taking tax exemption under this section.

One of the most secured and government-backed tax-saving options available to taxpayers in India is the **Section 54EC Bond.** These bonds, issued by specified public sector infrastructure institutions, offer individuals and entities a legitimate way to **reduce long-term capital gains tax liability** while ensuring the investment remains secure.

What Is Section 54EC Bond?

Section 54EC of the Income Tax Act, 1961 allows taxpayers to claim exemption from long-term capital gains (LTCG) arising from the sale of land or building or both, provided they have to reinvest such capital gain amount into "long term specified bonds" redeemable after five years and issued on or after the 1st April 2018, within a prescribed time.

These bonds are commonly known as Capital Gains Tax Exemption Bonds or 54EC Bonds. They are regarded as low-risk options because they are issued by highly rated public sector infrastructure companies backed by the Government of India.

Section 54EC is replaced by Section 85 under the The New Income Tax Act, 2025.

Section 85 of The Income Tax Act, 2025 also states that where the investment in such bonds has been taken into account for the purpose of exemption from long-term capital gains (LTCG) arising from the sale of land or building or both, no deduction under section 123 of The Income Tax Act, 2025, for any tax year shall be allowed for such investment.

Eligible Issuing Institutions

- HUDCO (Housing and Urban Development Corporation)
- REC (Rural Electrification Corporation)
- PFC (Power Finance Corporation)
- IRFC (Indian Railway Finance Corporation)
- IREDA (Indian Renewable Energy Dev Agency)

While all four have authorization, their bond issuances may vary depending on the year and government notifications.

Purpose of 54EC Bonds

The primary objective of introducing Section 54EC was to:

- Promote huge investment in India's infrastructure sector
- Provide taxpayers a safe, reliable, and transparent method of saving tax
- Promote the growth of economy due to the advancement of infrastructure sector
- Direct private investment toward long-term development outcomes and infrastructure programs.

By investing in these bonds, taxpayers not only save on capital gains tax but also contribute to the growth of critical national infrastructure.

Key Features of Section 54EC Bonds

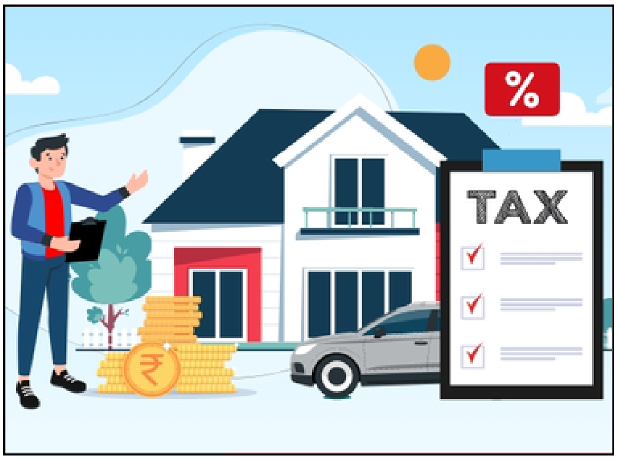
1. Tax Exemption Eligibility

To claim exemption under Section 54EC:

- The capital gain must arise from the **sale of long-term land or building.**
- The investment must be made **within 6 months** from the date of sale of the long term asset.
- The exemption amount equals the investment in the bonds, subject to a limit of **Rs.50 lakhs** per financial year.

2. Lock-in Period

54EC bonds come with a mandatory **5 years lock in period.** During this tenure, the investment cannot be redeemed or transferred.



If the investment made under Section 54EC is withdrawn or transferred before the lock-in period of five years as mentioned above, the capital gain exempted earlier will become taxable in the year of withdrawal, and the assessee will be liable to pay tax accordingly.

3. Interest Rate

These bonds typically offer an annual interest rate ranging from **5% to 5.75%**, depending on the issuer.

The interest is **taxable** and added to the investor's income. (currently it is 5.25%)

4. Minimum and Maximum Investment

- Minimum investment is generally Rs. 10,000.
- Maximum investment allowed for claiming tax exemption is **Rs.50 lakhs** in a financial year.

5. Mode of Holding

These bonds can be held in **dematerialized** or **physical certificate** form, subject to issuer availability.

How Section 54EC Helps Save Taxes

The tax exemption applies only to the **amount of capital gain invested.**

Here's a simple example to understand the whole concept of these bonds:

Mr. X sold a long-term commercial building on 10 January 2025.

After indexation, his long-term capital gain (LTCG) :Rs.80 lakhs.

He also sold shares during FY 2024-25 with a long-term gain of Rs.5 lakhs, but this cannot be claimed under Section 54EC, because 54EC applies only to gains from land or building, not shares or securities.

Mr. X must invest within 6 months from the date of sale of long term asset:

Sale date: 10 January 2025
6-month deadline : 9 July 2025

He must ensure all investments are completed before this date.

How the Rs.50 Lakh Yearly Limit Affects the Investment Plan

Section 54EC permits a **maximum investment of Rs.50 lakhs in a single financial year.**

Let's understand this with the above example of Mr. X:

In Mr. X's case, the 6-month investment window spans **two different financial years,** which creates a potential planning advantage.

- The property was sold in **FY 2024-25** (1 April 2024 to 31 March 2025).
- The 6-month deadline for investing under Section 54EC falls in **FY 2025-26.**

Because the investment window overlaps two financial years, Mr. X is allowed to structure his investment as follows:

- Invest **Rs.50 lakhs in FY 2024-25,** and
- Invest the remaining **Rs.30 lakhs in FY 2025-26,**

provided both investments are completed within the 6-month eligibility period.

This staggered approach is fully permissible under Section 54EC and is often used to maximize exemption benefits.

"Consequence of Delayed 54EC Investment"

If Mr. X fails to invest the first Rs.50 lakhs before 31 March 2025, he loses the advantage of splitting the investment across two financial years. Under Section 54EC, only Rs.50 lakhs can be invested per year, so any amount invested after 1 April 2025 will be counted entirely in FY 2025-26. As a result, although his total capital gain is Rs.80 lakhs, he can claim exemption on only Rs.50 lakhs, and the remaining Rs.30 lakhs will be fully taxable under the Section 112. (Now Section 197)

How to Invest in 54EC Bonds

- **Check Eligibility:** Ensure you are eligible to invest.
- **Choose Issuer:** Select from NHAI, REC, PFC, or IRFC as per your preference.
- **Application Method:** Apply online through the issuer's website/bank platform or you can also submit the application form offline.
- **Submit Required Documents:** Provide KYC documents such as **PAN card, Aadhaar card, address proof, passport-size photo,** and bank details for the verification.
- **Payment:** Make payment via cheque, DD, or online transfer depending on the application mode.
- **Bond Allotment:** Receive the bonds in your **De-mat account** or as a **physical certificate.**

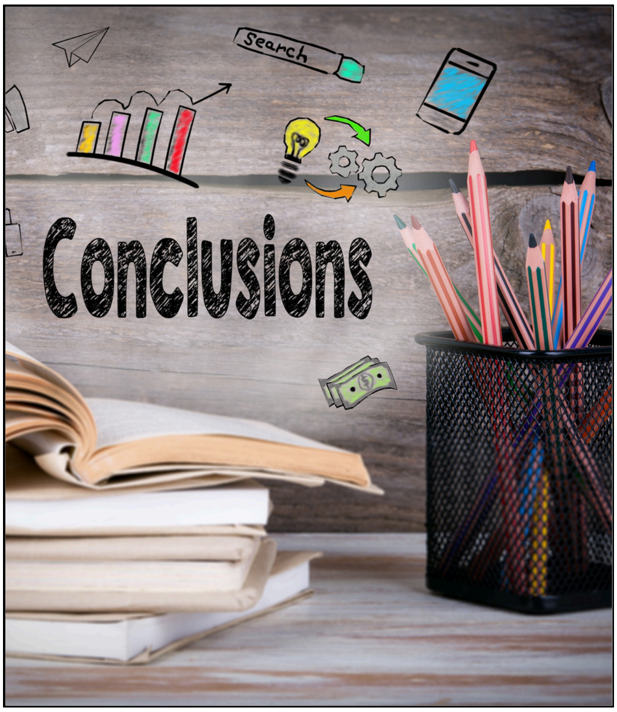
Who Should Invest in 54EC Bonds

- **Individuals with Capital Gains:** Ideal for anyone who has earned long-term capital gains, only from selling property, land, or buildings. (Not from selling shares, mutual funds or other securities.)
- **Investors Seeking Tax Exemption:** Suitable for those wanting to save capital gains tax under Section 54EC by reinvesting within 6 months of the sale of the long term asset.
- **Low-Risk Investors:** Investment in this type of bonds are beneficial for those who wants risk free returns without any headache.
- **People Who Can Hold for 5 Years:** This can be a better option for those who can patiently hold their investment in such bonds for minimum 5 years.
- **Retirees or Senior Citizens:** This is mostly preferred by the retired individual and senior citizen as they seek risk free returns and stable income.

Impact of the New Income Tax Act, 2025 on 54EC (Now Section 85)

As per The Income Tax Act, 1961, Long Term Capital Gains arising from the sale of land or building were taxable under Section 112 at the rate of 20% so the taxpayer could escape from this huge tax liability by investing such gains in 54EC Bonds.

In the Income Tax Act, 2025, Long Term Capital Gains arising from the sale of land or building is now governed under **Section 197** at the reduced rate of **12.5%**. Due to this reduction in LTCG tax rates, the overall tax benefit deriving from investment in 54EC Bonds (Section 85) has reduced. Under the previous Act, taxpayer was avoiding 20% of tax and now the exemption benefit can be claimed with the extent of 12.5% on LTCG as per Income Tax Act, 2025. If we compare both the Act, the benefits from the such investment plan is reduced by 7.5%.



CONCLUSION

Section 54EC Bonds are not just a tax saving bond, they are a smart way to secure your profits from the sales of long term assets i.e. land or building or both. By investing on time and following the annual limits as mentioned above, you can reduce your capital gains tax while showing interest in national infrastructure and joining hands in the advancement of the economy of the India. Escaping deadlines of investing in such bonds can lead to forfeiture of the tax benefits, so strategic planning is very crucial under this section to reinvest the capital gains for the purpose of tax exemption.

CA Sangam Aggarwal

Regional Council Member, NIRC of ICAI
National Vice President
International Navodaya Chamber of Commerce.

Revenue Recognition Under Ind As 115: A Practical Guide for Modern Business

SECTION 5: Detailed Judgements Involved in Each Step of Ind AS 115

Ind AS 115 is principle-based, not rule-based.

This means companies must apply **professional judgement** at many stages.

In real life, finance teams often spend more time interpreting contracts than passing entries.

This section explains the **key areas where judgement is required** and how organisations deal with them.

5.1 Judgements in Step 1: Identifying the Contract

Identifying a contract seems simple, but in practice, it can be tricky.

Many companies deal with verbal agreements, purchase orders, email approvals, and informal arrangements.

Major judgements include:

1. Determining Enforceability

Is the contract legally binding?

Some industries work on email confirmations or repeat purchase patterns.

Example:

A long-term distributor places orders every month without signing a fresh contract.

The company must decide whether this repeated arrangement forms an enforceable contract.

2. Assessing Collectability

Revenue can be recognised only when collection is "probable."

Judgement needed:

- Does the customer have good credit history?
- Is there financial stress?
- Are there past defaults?

Example:

Selling goods to a financially weak customer may require delayed revenue recognition until collectability is assured.

3. Modifications and Change Orders

Many contracts evolve over time.

Example:

In engineering or IT projects, customers add extra features mid-way.

Finance teams must decide whether it is:

- A **new contract**, or
- A **modification of the existing one**

This affects revenue timing.

5.2 Judgements in Step 2: Identifying Performance Obligations

Determining what is "distinct" can be highly subjective.

Key judgement areas:

1. Bundled products

Is the bundle one obligation or multiple?

Example:

Software + implementation + training + annual support.

Some companies treat them separately; others see them as an integrated solution.

2. Customisation

If the company significantly modifies the product for the customer, it may not be "distinct."

Example:

A software license that works only after custom coding → not distinct.

3. Implicit promises

Sometimes companies deliver more than what is written in the contract.

Example:

Free installation, free upgrades, free onboarding assistance.

These may become additional performance obligations depending on customer expectation.

5.3 Judgements in Step 3: Determining Transaction Price

The transaction price is rarely just the invoice amount.

Companies must estimate variable components and consider uncertainty.

Areas requiring judgement:

1. Variable consideration

This includes:

- Discounts
- Rebates
- Incentives

- Penalties
- Performance bonuses

Under Ind AS 115, companies must estimate these amounts **upfront.**

2. Choosing the estimation method

Two methods are allowed:

- Expected value method
- Most likely amount method

Companies must use the method that best predicts the final outcome.

3. Significant financing component

If payment is:

- Made far in advance, or
- Significantly deferred

...the company must adjust the transaction price for time value of money.

Example:

Customer pays ₹1 crore upfront for a service delivered over 4 years → financing component exists.

4. Consideration payable to customers

Cashbacks, vouchers, loyalty points, or dealer bonuses reduce the transaction price.

Judgement:

Estimating usage pattern and redemption rates.

5.4 Judgements in Step 4: Allocation of Transaction Price

When a contract has multiple performance obligations, allocation requires estimation.

Key judgement areas:

1. Determining standalone selling prices

If a company does not sell the goods/services separately, it must estimate the price.

Methods include:

- Adjusted market approach
- Cost-plus method
- Residual approach

2. Discounts allocation

If the customer gets a bundled discount:

- Should it be allocated equally?
- Or only to specific obligations?

Example:

Handset + service plan bundles often require detailed allocation based on relative standalone prices.

3. Variable consideration allocation

In some cases, variable consideration relates only to a specific performance obligation.

Example:

A performance bonus paid only for implementation work → allocate only to implementation, not to the software license.

5.5 Judgements in Step 5: Recognising Revenue

This step involves the highest level of judgement.

1. Whether revenue is recognised over time or at a point in time

The core judgement is:

Does the customer receive benefit as work happens?

Construction, AMC, and long-term IT projects usually recognise revenue over time.

Retail sales, hardware sales, and standalone products usually recognise at a point in time.

2. Measuring progress

For over-time revenue, companies must measure progress using:

- Cost-to-cost method
- Surveys of work completed
- Units produced or delivered
- Engineering assessments
- Milestone achievements

Choosing the right method requires significant judgement.

3. Contract assets vs receivables

If a company completes work but cannot bill yet, it creates a **contract asset,** not a receivable.

Judgement is needed to determine when billing rights arise.

4. Customer acceptance

In some cases, control transfers only when the customer approves the work.

Example:

A software customization project may be complete technically but cannot be recognised as revenue until customer acceptance testing is done.

5. Handling contract modifications

If scope or price changes, the company must decide:

- Does the modification create a new contract?
- Or is it part of the existing contract?

This affects revenue timing and allocation.

Summary of Section 5

Ind AS 115 requires companies to apply judgement at almost every step.

The standard provides the framework, but real-life application depends on a deep understanding of the contract, customer expectations, and business model.

Finance teams must work closely with:

- Sales
- Operations
- Legal
- Project managers
- Business analysts

…to ensure revenue is recognised correctly.

SECTION 6 - Identifying Performance Obligations under Ind AS 115

One of the most important steps in the revenue recognition process is **identifying performance obligations.** This step decides when and how revenue will be recognized. In practice, many companies struggle with this because products and services are often bundled together, discounted, or dependent on each other.

Ind AS 115 requires entities to **identify each promise** made to the customer and determine whether it is a **distinct performance obligation.**

6.1 What Is a Performance Obligation?

A performance obligation is:

- A **promise** in a contract to transfer a good or service
- That is **distinct, meaning** the customer can benefit from it on its own or with other resources
- And is **separately identifiable** within the contract

In simple terms:

Each item or service the customer is paying for — if distinct — becomes a performance obligation.

6.2 When Is a Good or Service "Distinct"?

Ind AS 115 provides a two-step test:

(A) Customer Can Benefit from the Good or Service

This means:

- The item has standalone utility
- The customer could buy it separately
- Or use it with other items already owned

Examples:

- A mobile phone alone → distinct
- Installation service alone → distinct
- Spare parts sold separately → distinct

(B) The Good or Service Is Separately Identifiable

This means the item is **not heavily integrated** with other items.

Indicators a good/service is not separately identifiable:

- The seller provides a **significant integration service**
- Goods are **highly interdependent**
- One item significantly modifies/customizes another

Example:

A software license that needs heavy customization → **NOT distinct.**

A ready-made software plus simple installation → **distinct.**

6.3 Common Practical Scenarios in India

1. Telecom Companies

Bundle: Mobile handset + Data plan

- Handset → distinct
- Data plan → distinct
  Revenue is split between the handset and the plan.

2. Construction and Real Estate

Contract for:

- Base construction
- Interior work
- Custom design
- Maintenance

Often these are **integrated,** resulting in **one performance obligation,** unless clearly separable.

3. Software Companies

Licenses + Implementation + AMC

- License (distinct)
- Implementation (may or may not be distinct depending on level of customization)
- AMC (distinct)
  Each is assessed separately.

4. Manufacturing

Sale of machinery + installation

If installation is simple → separate obligations

If installation is complex and machinery cannot function without it → single obligation

6.4 Promises That Are NOT Performance Obligations

Not everything stated in a contract automatically becomes a performance obligation.

Examples:

- **Quality assurance** warranties (these are normal warranties, not separate obligations)
- **Marketing incentives** with no real value
- **Administrative tasks** (sending invoices, documentation)

These do not transfer value and therefore are not obligations.

6.5 Combination of Goods/Services into One Obligation

Sometimes goods/services must be combined.

Examples:

- EPC contracts
- Custom-built machinery
- Large building projects
- Software requiring deep customization

In these cases, the customer receives a single integrated output, so revenue is recognized using % completion or over time.

6.6 Practical Challenges Companies Face

1. Bundled Pricing

Indian companies often bundle goods without separate pricing.

Solution: allocate transaction price based on standalone selling price.

2. "Free" Items

Free maintenance, service visits, or accessories may actually be separate obligations.

They must be valued and part of revenue allocation.

3. Customization Level

The challenge is deciding whether customization is:

- Minor → Separate obligation
- Significant → Combined obligation

4. Multiple Contract Modifications

Changes in scope require re-evaluation of obligations each time.

6.7 Documentation Required in Practice

To apply Ind AS 115 correctly, auditors expect documentation such as:

- Contract analysis sheet
- List of promises
- Distinctness test (benefit + separable)
- Allocation basis
- Analysis of warranties
- Notes on integration/customization
- Internal approvals

This documentation helps defend the revenue treatment during audits.

6.8 Summary

Identifying performance obligations is the **foundation** of Ind AS 115.

It ensures that:

- Revenue is recognized at the correct time
- Bundled products are properly split
- Complex contracts are handled consistently
- Financial statements maintain integrity

SECTION 7

Determining the Transaction Price

Once the performance obligations are identified, the next step under Ind AS 115 is to determine the **transaction price**—the amount of consideration the entity expects to receive in exchange for transferring goods or services.

In simple terms:

Transaction price is the total money (or value) the company expects from the customer.

But in reality, this amount is often not straightforward. Discounts, incentives, bonuses, penalties, financing components, and variable pricing make it more complex.

This section explains how entities determine the transaction price in practical situations.

7.1 What Is the Transaction Price?

The transaction price is the **expected consideration** an entity will receive, considering:

- Fixed amounts
- Variable amounts
- Non-cash consideration
- Significance of financing components
- Any consideration payable to customers

It reflects the actual economic substance of the transaction — not just the invoice amount.

7.2 Components of Transaction Price

1. Fixed Consideration

These are amounts clearly agreed upon in the contract.

Examples:

- Product sold at ₹1,00,000
- Fixed installation fee ₹10,000
- Subscription service at ₹2,000/month

Fixed consideration is straightforward and forms the base of the transaction price.

2. Variable Consideration

Many contracts include conditions that affect the final price.

Variable consideration may include:

- Volume discounts
- Early payment discounts
- Rebates
- Price incentives
- Performance bonuses
- Penalties for delays
- Sales returns
- Usage-based fees

Ind AS 115 requires companies to **estimate variable consideration upfront** using one of two methods:

(A) Expected Value Method

Suitable when the company has multiple contracts with similar customers.

(B) Most Likely Amount Method

Used when the outcome is binary (bonus achieved or not achieved).

Example:

A contractor will receive ₹5 lakhs bonus only if the project is completed before deadline.

Most likely amount method is used.

7.3 Constraint on Variable Consideration

Ind AS 115 is conservative with revenue.

Companies must include variable consideration in transaction price **only if it is highly probable that revenue will not reverse later.**

This is called the **"constraint" requirement.**

Example:

A company expects a bonus from a government contract but approval is uncertain.

Revenue is **NOT recognized** until probability becomes high.

7.4 Significant Financing Component

Sometimes customers pay:

- In advance (subscription fees, real estate booking)
- In arrears (deferred payment, EMI sale)

If timing provides a **significant financing benefit** to either party, interest must be separated from revenue

Indicators of significant financing:

- Long gap (generally more than 12 months)
- Price difference between cash and credit terms
- Customer benefit from deferring payment

Not counted as financing:

- Advance payments purely for security
- Short gaps (less than 12 months)
- Customer payments tied to progress milestones

7.5 Non-Cash Consideration

Transaction price must include:

- Goods given by the customer
- Services provided by the customer
- Barter transactions

Example:

A customer provides raw material instead of paying part of the fee.

Its **fair value** must be included in revenue.

7.6 Consideration Payable to Customers

Sometimes businesses pay customers to promote, sell, or buy their products.

Example:

- Credit notes
- Cashback
- Trade schemes
- Shelf-display fees paid to retailers

These payments are treated as **reduction of revenue,** not expenses, unless the payment is for a distinct service received from the customer.

7.7 Practical Industry Examples

1. FMCG Industry

Companies give:

- Trade discounts
- Volume rebates
- Schemes

This creates variable consideration.

Revenue recognized only after assessing "high probability" of no reversal.

2. Telecom Industry

Usage-based charges (data usage, SMS packs) require estimation of variable revenue.

Bonus data packs are treated as reduction of transaction price, not marketing expense.

3. Real Estate

Customers often pay in instalments over long periods.

This may create a **significant financing component.**

Revenue must be discounted using a financing rate.

4. EPC/Construction

Contracts often include:

- Performance bonuses
- Liquidated damages
  Both treated as variable consideration.

Entity must estimate whether bonuses will be earned or penalties will apply.

7.8 Practical Challenges Companies Face

1. Estimating variable consideration accurately

Businesses often struggle due to:

- Complex sales schemes
- Unpredictable customer behaviour
- Dependence on external approvals

2. Separate accounting for financing components

Many companies miss discounting long-term receivables.

3. Assessing whether incentives are for customers or for a distinct service

This is judgment-heavy.

4. Documentation

Auditors expect detailed working papers explaining calculations.

7.9 Summary

Determining the transaction price is one of the most judgmental areas under Ind AS 115.

Companies must consider all components:

- Fixed and variable pricing
- Rebates, bonuses, penalties
- Financing effects
- Non-cash consideration
  Customer payments

Conclusion

Ind AS 115 has fundamentally changed the way companies look at revenue. It is no longer just about recording sales when an invoice is raised, or when cash is received. Instead, the standard requires businesses to understand their contracts, identify each promise made to the customer, and recognise revenue only when value is truly delivered.

For many companies, this shift has been challenging. It demands judgement, documentation, and coordination between finance, sales, procurement, and legal teams. Yet, it has also brought clarity, discipline, and consistency across industries. When applied correctly, Ind AS 115 ensures that financial statements reflect the real economics of a transaction, not just its paperwork.

From identifying performance obligations to estimating variable consideration, from determining transaction price to evaluating contract modifications, every step requires thoughtful analysis. In practice, the goal is simple:

Revenue should represent the transfer of goods or services—not assumptions, not timing differences, and not outdated habits.

Indian companies are gradually adopting a more structured approach to contracts, pricing, and delivery because of this standard. As a result, revenue recognition is becoming more transparent, comparable, and investor-friendly.

Ultimately, Ind AS 115 is not just an accounting rule—it is a framework that promotes fairness, accountability, and a deeper understanding of business performance. When implemented carefully, it strengthens trust between companies, auditors, regulators, and most importantly, the users of financial statements.

CMA Puja Mishra

Editorial Board Member
The Worldonomics Times

हाउसिंग एंड अर्बन डेवलपमेंट कॉर्पोरेशन लिमिटेड
(भारत सरकार का उपक्रम)

Housing & Urban Development Corporation Limited
(A Government of India Enterprise)

आज़ादी का अमृत महोत्सव

एम नागराज
निदेशक (कॉरपोरेट प्लानिंग)

M. NAGARAJ
Director (Corporate Planning)

MESSAGE

Dear Shri Sandeep Kumar,

I extend my warmest congratulations to you on the impending launch of Global Finance and Economics Magazine: The Worldonomics Times on May 5th! This milestone marks the beginning of what promises to be an exciting journey in the realm of global finance and economics journalism.

As our world becomes increasingly interconnected, the need for a comprehensive and insightful resource in the field of finance and economics has never been greater. Your magazine's dedication to providing a platform for experts to share their insights is commendable and much needed in today's complex economic landscape.

I have no doubt that The Worldonomics Times will quickly establish itself as a key resource for policymakers, industry professionals, academics, and anyone with a keen interest in understanding the intricacies of global finance and economics. Your commitment to delivering high-quality, well-researched content will undoubtedly set a new standard in the industry.

I eagerly anticipate the inaugural issue and look forward to the valuable contributions and perspectives that The Worldonomics Times will bring to the forefront of economic discourse.

Once again, congratulations on this significant achievement, and I wish you all the best for a successful launch and a prosperous future ahead.

(CMA - M. NAGARAJ)

AN ISO 9001:2015 CERTIFIED COMPANY

CIN : L7489DL1970GOI005276
E-mail : dcp@hudco.org

Follow us on
@hudcolimited

एच.ई.सी.

ISO 9001:2008 Company

Rajesh Kumar Dwivedi
Director (Finance)

स्वच्छ भारत
एक कदम स्वच्छता की ओर

Heavy Engineering Corporation Ltd.
(A Govt. of India Enterprise)
P.O.- Dhurwa, Ranchi - 834 004 Jharkhand (India)
Phone : 0651-2401372, 2400575 (O)
Fax : 0651-2400574 (O)
Mob. : 9650572233
E-mail : dir_fin@hecltd.com

MESSAGE

Dear Shri Sandeep Kumar,

I take this opportunity to heartily congratulate you on publishing "The Worldonomics Times", which I really feel is a hands-on treasure of useful information.

Today's world is rapidly changing and inter-woven with diverse complexities. In such a global environment, authentic and timely information is a powerful tool which I am sure will be always provided by "The worldonomics Times". I am sure, the adage that "*The Pen is mightier than the Sword*" will be once again be proven right with your magazine.

Congratulations, once again and my Best wishes for this wonderful knowledge endeavour!

(CMA Rajesh Kumar Dwivedi)

BLESSING SUPPORT

CMA Sanjay Jindal

Director Finance | Engineers India Limited

Dear Mr. Sandeep Kumar,
With the launch of The Worldonomics Times, professionals worldwide are poised to embark on a journey of enlightenment and empowerment. In today's fast-paced economic landscape, the need for up- to-date insights and innovative strategies is more crucial than ever. As Director (Finance), I recognize the significance of continuous learning and informed decision-making. This magazine promises to be a comprehensive resource, offering valuable insights and actionable strategies to navigate the challenges and opportunities ahead. The Worldonomics Times is not just a publication; it's a beacon of innovation in economic discourse. Through cutting-edge analysis, thought-provoking articles, and expert commentary, it will serve as a trusted companion for professionals across various sectors. Leveraging the latest technologies, the magazine ensures accessibility and engagement for all readers, regardless of background or expertise. Beyond economics, The Worldonomics Times will explore intersections of finance with technology, sustainability, and social responsibility. By fostering dialogue and collaboration across diverse fields, it will inspire innovative solutions to global challenges. I am proud to be associated with this initiative, and I extend my deepest gratitude to the editorial team, contributors, partners, and supporters who have worked tirelessly to bring this vision to life. I offer my sincerest blessings to all those who will embark on this journey of enlightenment and empowerment, fueling innovation and success in the ever-evolving world of economics. Impressive Initiative! Best Wishes to you and your team for resounding success on this fantastic effort.

CMA Hrishikesh Kumar

Executive Director (Finance) | NBCC (India) Limited

Dear Shri Sandeep Kumar,
At the outset I would like to congratulate you for taking the initiative for publishing this magazine “The Worldonomics Times”. In this era of rapid changing economic environment vis-à-vis the pressure on business to sustain, the importance of seamless transfer of information and knowledge cannot be underestimated which I hope would be fulfilled by your magazine in future.I must say this is a great initiative by you and your team in this regard. All the est for your endeavor.

CMA Yogendra Prasad Shukla

Director Finance | HOCL - Hindustan Organic Chemicals Limited

Dear CMA Sandeep Kumar Ji,
I extend my heartfelt congratulations on the launch of "The Worldonomics Times." Your dedication to providing a platform for insightful economic knowledge is truly commendable. In today's- paced economic, the significance of facilitating the smooth flow of information and wisdom cannot be overstated, and I am confident that your magazine will excel in meeting this crucial need. Your initiative, alongside your team, is truly praiseworthy, and I foresee "great success for “The Worldonomics Times" in the days ahead. Your commitment to empowering minds through economic understanding is inspiring. Best regards.

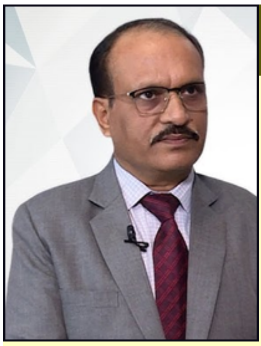
BLESSING SUPPORT

CMA Yash Paul Bhola

Former Director (Finance)| NFL - National Fertilisers Limited

Dear INCOC Team Members,

I congratulate and appreciate the efforts by one and all in bringing out Global Finance and Economics Magazine, "The Worldonomics Times". This milestone marks the beginning of an exciting journey in the realm of global finance and economics journalism. As our world becomes increasingly interconnected, and regulatory framework is fast getting changed and updated, the need for a comprehensive magazine in finance field cannot be over emphasised. This magazine is dedicated to providing a platform for periodical up-dation of the developments across the globe and experts to share their insights. It is intended to establish itself as a key resource for policymakers, industry professionals, academics, and anyone with a keen interest in understanding global finance and economics. Once again, I congratulate and wish you all the best for a successful launch of the magazine and a prosperous future ahead.



CMA Gaurang Dixit

Former Chairman-cum-Managing Director |
NSIC - National Small Industries Corporation

Dear Shri Sandeep Kumar,

At the onset, I applaud the initiative of the 'International Navodaya Chamber of Commerce' to come out with a magazine 'The Worldonomics Times', which will provide the relevant information and knowledge to the all in this diverse global market. In the present complex business / economic scenario, the whole world market is like a field open for all players to play thereon. This global market is having abundant opportunities and to become a successful entrepreneur in such complex economic environment, the need for having relevant information and knowledge is of paramount significance. Your endeavour to come out with the magazine 'The Worldonomics Times' will certainly help to suffice this requirement. I must congratulate to you and your team for this endeavour. With best wishes.

CMA R C Gupta

Former Executive Director (Finance & Accounts)| GAIL (India) Ltd.

Dear Shri Sandeep Ji,

I have gone through the May 2024 issue of The Worldonomics Times and found it very informative. My heartfelt congratulations on the launch of a world class magazine in the area of Cost Management, Financial Management, Financial Planning, Taxation and World Economic Affairs. The coverage in the magazine is very wide & excellent and is based on the theme of Global Perspective with Local Relevance, in-depth data driven journalism and accessibility of the magazine in print as well as digital formats. It will empower the readers with well researched articles for ready reference, decision making & knowledge enhancement. I wish all the best to you and your team of International Navodaya Chamber of Commerce (INCOC) for bringing the magazine on regular basis with full of information of world economic affairs for use by all professionals. With Best regards.

BLESSING SUPPORT

Shri Jyoti Prakash Gadia

Managing Director | Resurgent India Limited

Dear Sandeep Ji,

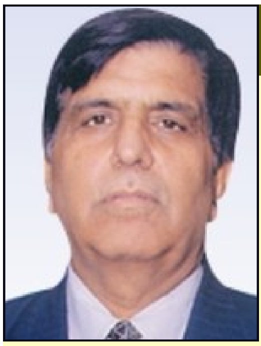
Congratulations on the launch of The Worldonomics Times! This new publication promises to be a vital resource in financial journalism and stands to reshape our grasp of global financial landscapes. The Worldonomics Times will undoubtedly be an indispensable source for thorough analyses, covering the nuanced intersections of global economics and market dynamics. Your magazine is uniquely positioned to serve the needs of business leaders, policymakers, and those with a keen interest in the complexities of global finance. We eagerly await the fresh perspectives and insights that The Worldonomics Times will bring to the complex world of global finance. Best wishes for your journey ahead!

CMA Ramesh Kumar

Chief General Manager | Power Grid Corporation Of India

Dear Shri Sandeep Kumar,

With great pleasure we extend our good wishes on the launch of The Worldonomics Times. This publication is poised to become a cornerstone in the landscape of global finance and economics, offering deep insights and valuable perspectives. Your commitment to excellence in disseminating knowledge is not only commendable but vital in these complex economic times. We eagerly anticipate the success and influence your magazine will undoubtedly achieve. Warm regards.



Shri BK Sabharwal

Chairman, Capital and Commodity Market Committee, PHDCCI Ex-President CPAI, Ex-chairman FISE, Ex-Director |Delhi Stock Exchange

Dear Sandeep Kumar,

Congratulations on the launch of The Worldonomics Times! Your dedication to global finance journalism is commendable. This milestone marks the beginning of an insightful journey. In our interconnected world, timely updates on regulatory changes are vital, and your magazine promises to fulfill this need. Dedicated to providing expert insights and periodic updates, it aims to become a key resource for policymakers, industry professionals, and academics. Your leadership in this initiative is inspiring. Here's to a successful launch and a prosperous future ahead. Best regards.

CMA Vijay Kumar Agarwal

GM (Finance) | ONGC Videsh

Dear Shri Sandeep Ji,

It's my great pleasure to note "The Worldonomics Times" monthly magazine launching by "International Navodaya Chamber of Commerce (INCOC). The various Global Perspectives with relevant data have been covered which are relevant from our local perspective. The contents of magazine in coming days will be way forward in knowledge enhancement as well as for better understanding in correlating the global economics with local need. Congratulations CMA Sandeep ji & Team for such an initiative which will surely provide the tailored world economic information.

THE WORLDONOMICS TIMES

TOPICS INVITED

Cover Stories on the topics given below are invited for 'The Worldonomics Times' for the four forthcoming months

Month		Theme		Topics
February 2026	Theme	Financing Strategies and Financial Health	Topics	**Alternative Financing:** Exploring options beyond traditional bank loans, such as P2P lending, angel investors, venture capital, and government schemes. **Effective Cashflow Management:** Tools and techniques for forecasting, managing receivables, and optimizing payables. **Budgeting for Scalability:** Creating budgets that support planned growth and R&D without overextending. **Navigating Tax Compliance:** A simplified guide to MSME tax benefits, deductions, and regulatory changes for the upcoming fiscal period.
March 2026	Theme	Export Promotion and International Business Opportunities	Topics	**Identifying Export Markets:** Analyzing global demand and selecting the right countries for specific products/services. **Logistics and Supply Chain:** Understanding international shipping, customs, and managing an effective global supply chain. **Incentives and Trade Agreements:** Utilizing government export promotion schemes and taking advantage of Free Trade Agreements (FTAs). **Cultural Competence:** Tips for successful negotiation and communication with international clients and partners.
April 2026	Theme	Talent Management, Skilling, and HR Excellence	Topics	**Attracting and Retaining Talent:** Strategies for small businesses to compete with larger companies for skilled employees. **Employee Upskilling and Training:** Low-cost ways to invest in employee growth, focusing on digital and soft skills. **The Future of Work:** Adapting to hybrid models, managing remote teams, and ensuring productivity. **MSME Workplace Culture:** Building a positive, resilient, and inclusive environment that drives innovation and loyalty.
May 2026	Theme	Sustainable Growth and Future-Proofing MSMEs	Topics	**Green Business Transition:** Practical steps for MSMEs to adopt eco-friendly practices and prepare for CBAM. **Circular Economy Opportunities:** Turning waste reduction in to new revenue through recycling and sustainable sourcing. **ESG for Small Business:** Understanding ESG essentials to secure large contracts and investor confidence. **Building Business Resilience:** Future-proofing businesses against supply chain, climate, and policy risks.

The Worldonomics Times invites leading professionals, like yourself, to contribute expert articles (800-1,200 words) on global economics, finance, and policy for an upcoming issue.

We are seeking original insights and analysis from experts in above topics to enrich our readership of business leaders and policymakers.

All submissions must be accompanied by recent, high-resolution photographs or supporting visual assets. Please submit your completed article and visuals by 20th of following month to support@incoc.in. We look forward to featuring your valuable perspective.

www.worldonomics.in

International Navodaya Chamber of Commerce

www.incoc.in

INCOC

International Navodaya Chamber of Commerce

INCOC LANDMARK LEADERSHIP AWARD

DATE : 22nd February 2026

Prominent Personalities to Give & Receive Awards

- Chief Guest
- Member of Parliament
- Corporate Leaders
- Professional Leaders and Jury
- PSUs & Bankers
- Media and Entertainment
- Entrepreneurs
- Professional Students

SANDEEP KUMAR (FCMA, CA)
National President
International Navodaya Chamber of Commerce

Register for Award
www.worldonomics.in/illa2026/

MSME Leadership Summit 2026

INCOC

PROFESSIONAL YOUTH FOR

विकसित भारत

Supported By:

गेल GAIL

EIL

हडको hudco A NAVRATNA CPSE

Tally

IDBI BANK

International Navodaya Chamber of Commerce

www.incoc.in

INCOC

Head Office
Alankrit Society A 31, Plot A1, Vishwas Nagar Delhi 110032

Tel: +91 11 69268366

National President
CA CMA Sandeep Kumar
ceo@incoc.in

National Vice President
CA Sangam Aggarwal
sangam@incoc.in

Email Us
We'll respond to your inquiry as soon as possible.
info@incoc.in

Website
www.incoc.in

Connect With Us
Ms Neha Sharma
support@incoc.in

International Navodaya Chamber of Commerce (INCOC)

Welcome to the International Navodaya Chamber of Commerce (INCOC), a dedicated catalyst for positive change, empowerment, and community development. We are committed to enhancing brand value, nurturing essential skills, and facilitating societal growth through a collaborative and community-centric approach.

Our Mission

At INCOC, our mission is to harness the collective potential of individuals and businesses to create a lasting impact. We believe in the power of collaboration, empowerment through knowledge, and a community-centric approach to address local needs and promote inclusivity. Our initiatives are designed to inspire actionable impact, foster continuous learning and adaptation, and contribute to building a brighter future.

How We Operate

- **Collaborative Synergy:** We thrive on collaboration, bringing together diverse minds, expertise, and resources to foster an environment where ideas flourish and innovation thrives.
- **Empowerment through Knowledge:** Knowledge is the cornerstone of growth. At INCOC, we provide access to valuable insights, expert advice, and resources that empower individuals and businesses to make informed decisions and drive positive change.
- **Community-Centric Approach:** Communities are at the heart of change. Our initiatives are designed to address local needs, promote inclusivity, and create a sense of belonging, tailoring our efforts to have a meaningful impact where it's needed most.
- **Actionable Impact:** Our programs inspire action and create tangible results, from skill development workshops to societal initiatives that drive positive change, focusing on making a real difference.
- **Continuous Learning and Adaptation:** We embrace continuous learning and adaptation to stay relevant in a rapidly changing landscape, ensuring that our strategies remain effective and aligned with the needs of the times.