VOL. 54 ISSUE 4

WIRC BULLETIN

ENGLISH MONTHLY I APRIL 2026 I PAGES 64 I PRICE RS.5/- I RNI NO. 22703/72

Cybersecurity, Forensic Audit, and Digital Vigilance

ICMAI
THE INSTITUTE OF
COST ACCOUNTANTS OF INDIA
भारतीय लागत लेखाकार संस्थान
Statutory Body under an Act of Parliament
(Under the jurisdiction of Ministry of Corporate Affairs)
WESTERN INDIA REGIONAL COUNCIL

Follow us on:

Glimpses from Student's Regional Cost Convention 2026 organised by WIRC on 17th & 18th March, 2026 at Surat

CMA Ashvin Ambaliya, Treasurer ICMAI - Surat South Gujarat Chapter, CMA Kishor Vaghela, Chairman - ICMAI Surat South Gujarat Chapter & Co-Convener, SRCC, CMA Chaitanya Mohrir, Secretary, ICMAI - WIRC, CMA (Dr.) Dhananjay V Joshi, Past President - ICMAI, CMA Neeraj D Joshi, Vice President - ICMAI, CMA TCA Srinivasa Prasad, President ICMAI, Guest of Honour Shri Nikhil Madrasi, President, SGCCI, Chief Guest Shri Hardik Kothiya, Chairman & Joint Managing Director Rayson Solar Ltd, CMA Mihir Vyas, Chairman ICMAI-WIRC, CMA Nanty Shah, Vice Chairman - ICMAI WIRC & Convener- SRCC, Student Committee, Chairman, ICMAI-WIRC

CMA TCA Srinivasa Prasad, President ICMAI alognwith CMA Mihir Vyas, Chairman ICMAI-WIRC felicitated Chief Guest Shri Hardik Kothiya.

CMA Neeraj D Joshi, Vice President - ICMAI alongwith CMA Nanty Shah, Vice Chairman - ICMAI WIRC felicitated Guest of Honour Shri Nikhil Madrasi, President, SGCCI

CMA Chaitanya Mohrir, Secretary, ICMAI - WIRC felicitated CMA TCA Srinivasa Prasad, President ICMAI

CMA Kishor Vaghela, Chairman - ICMAI Surat South Gujarat Chapter & Co-Convener, SRCC felicitated CMA Neeraj D Joshi, Vice President - ICMAI.

CMA Ashvin Ambaliya, Treasurer ICMAI - Surat South Gujarat Chapter felicitated CMA (Dr.) Dhananjay V Joshi, Past President - ICMAI

CMA Mahesh Bhalala, Managing Committee Member - Surat South Gujarat Chapter, CMA Amit Apte, Past President - ICMAI & Session Chairman, Speaker Dr. Ankit Shah and CMA Manisha Agarwal, Regional Council Member - ICMAI WIRC during Technical Session I

CMA Mahendra Bhombe, RCM, WIRC, CMA Vipin Patel and CMA Deepali Lakdawala Moderator for CMA Skillsprint Hackathon alogwith Participated Students.

Shri Nitinbhai Bhajiyawala Former President B.J.P - Surat City Chief Guest for CMA Srujan - Talent Competition is being felicitated by CMA Neeraj D Joshi, Vice President - ICMAI

View of Students Participated for Mock Parliament alongwith CMA (Dr.) Sanjay Bhargave and CMA Amey Tikale, Jury members.

Table of CONTENT

Vision Statement

"The Institute of Cost Accountants of India would be the preferred source of resources and professionals for the financial leadership of enterprises globally."

Mission Statement

"The Cost and Management Accountant professionals would ethically drive enterprises globally by creating value to stakeholders in the socio-economic context through competencies drawn from the integration of strategy, management and accounting."

From the Desk of Chairman

CMA Mihir Narayan Vyas

Chairman ICMAI -WIRC

Dear Esteemed Members and Students,

With great enthusiasm and renewed determination, we step into the New Financial Year 2026–27, a phase that symbolizes fresh opportunities, progressive vision, and collective growth for our profession. This auspicious beginning is further illuminated by the spirit of Akshay Tritiya, a festival that signifies eternal prosperity, success, and new beginnings. Traditionally associated with wealth and auspicious investments, Akshay Tritiya also reminds professionals like us to invest in knowledge, ethics, and continuous learning—assets that yield infinite returns. As Cost and Management Accountants, our commitment to value creation, integrity, and sustainable growth aligns deeply with this timeless philosophy of "Akshay" — that which never diminishes.

This month's bulletin theme, "Cybersecurity, Forensic Audit & Digital Vigilance," is both timely and critical in today's rapidly evolving digital economy. With increasing digitalization, India is witnessing a surge in cyber threats, financial frauds, and data breaches. Recent regulatory developments, enhanced focus on data protection frameworks, and the growing emphasis on digital governance have made cybersecurity and forensic audits indispensable. CMAs today are not just financial strategists but also custodians of digital integrity. Our role extends to ensuring robust internal controls, risk mitigation, fraud detection, and strengthening digital vigilance systems. As the nation progresses towards a digitally empowered economy, our profession must lead from the front in safeguarding trust and transparency.

On the national front, India continues to demonstrate strong economic resilience with policy reforms, infrastructure development, and a sustained push towards digital transformation. The government's focus on compliance, transparency, and ease of doing business further enhances the relevance of our profession in nation-building. As India moves towards the vision of Viksit Bharat@2047, CMAs will play a pivotal role in shaping accountable and efficient economic systems.

I am delighted to share that the **Students' Regional Cost Convention (SRCC) 2026** was successfully organized by WIRC of ICMAI on 17th & 18th March 2026 at Platinum Hall, SIECC Auditorium, Surat, hosted by the ICMAI Surat Chapter. With participation from over 800 enthusiastic CMA students, the convention was a vibrant platform for learning, networking, and inspiration. The event was graced by Chief Guest Shri Hardik Kothiya, Chairman & Joint Managing Director, Rayson Solar Ltd, and Guest of Honour Shri Nikhil Madrasi, President, SGCCI. The sessions were thoughtfully curated to empower students with industry insights, professional guidance, and a forward-looking perspective, making it a truly enriching experience.

Further strengthening our professional commitment, ICMAI successfully organized the **National Seminar on Cost Audit** on 10th April 2026 at Yashwantrao Chavan Centre, Nariman Point, Mumbai, on the theme "Value, Vishwas and Vision." The seminar aimed at deliberating the evolving role of cost audit in enhancing transparency, accountability, and efficiency in the economy. We were honoured by the **gracious presence of Hon'ble Shri Jishnu Dev Varma, Governor of Maharashtra, as the Chief Guest.** With participation from over 400 professionals & CMA Aspiriants, the seminar provided valuable insights and reaffirmed the significance of cost audit in achieving the national vision of Viksit Bharat@2047.

I am also pleased to inform that the **Advanced Skill Training Programme (ASTP) for December 2025 qualified CMA** candidates was successfully conducted by the Career Counselling & Placement Committee in association with WIRC. A total of 261 newly qualified CMAs completed this intensive training, equipping them with practical knowledge, industry readiness, and professional excellence. This initiative reflects our commitment to nurturing future-ready professionals.

The **Campus Placement Programme for newly qualified CMAs (December 2025 term)** is scheduled from **11th to 13th May 2026 in Mumbai.**

I strongly encourage members, corporates, and industry leaders to actively participate and support this initiative by providing opportunities to our talented professionals, thereby strengthening the industry-academia bridge.

In line with our focus on future skills, the ICMAI AI Strategy & Capacity Building Board organized "**CMA AI Pravesh** – Deep-Dive into Artificial Intelligence and Machine Learning for Finance and Cost/Management Accounting" from 3rd to 6th April 2026 at the WIRC Office. The sessions conducted by CMA Rahul S. Dharne and Ms. Rahee Walambe were highly insightful, equipping participants with practical understanding of AI applications in finance. Such initiatives are crucial as we embrace technological transformation in our profession.

Looking ahead, WIRC of ICMAI is organizing "मंथन – **3rd Regional Tax Conclave 2026" on 26th April 2026 at Bhilai**, centered on the theme "Strengthening Economic Growth through Tax Reforms and Compliances." This conclave aims to provide a platform for knowledge exchange, policy discussion, and professional development in the domain of taxation. I urge all members to actively participate and benefit from this significant event.

As we move forward in this new financial year, let us reaffirm our commitment to excellence, innovation, and ethical practices. Together, we can contribute meaningfully to the growth of our profession and the nation.

Wishing you and your family prosperity, good health, and success on the auspicious occasion of Akshay Tritiya and throughout the year ahead.

"Arise, awake, and stop not till the goal is reached."
— Swami Vivekananda

Warm regards,
CMA Mihir Narayan Vyas
Chairman
Western India Regional Council of
The Institute of Cost Accountants of India

Written by,

CMA Nanty Nalinkumar Shah

Vice Chairman ICMAI - WIRC &
Chairman, Editoral Board - WIRC Bulletin

With the dawn of the new financial year 2026–27, we step forward with renewed enthusiasm, sharper vision, and an unwavering commitment to excellence. The evolving business landscape driven by rapid digital transformation calls for professionals who are not only financially astute but also technologically vigilant and ethically resilient. It is in this spirit that we present the April edition of the WIRC Bulletin, centered around the compelling and timely theme: "Cybersecurity, Forensic Audit & Digital Vigilance."

In an era where digital transformation is redefining business operations, the risks associated with cyber threats, data breaches, and financial frauds have escalated manifold. Organizations today are not only expected to create value but also to protect it through robust governance mechanisms. This evolving landscape demands CMAs to go beyond traditional roles and emerge as strategic guardians of value, equipped with expertise in cyber risk assessment, forensic auditing, and digital vigilance.

Cybersecurity is no longer just an IT concern - it is a critical business imperative. Forensic audit has evolved as a powerful tool in detecting and preventing fraud, while digital vigilance ensures continuous monitoring and safeguarding of organizational assets. Together, these domains form a comprehensive shield against emerging risks, enabling professionals to contribute meaningfully to sustainable and resilient growth.

This edition is a complete knowledge compendium featuring insightful articles such as Data Breaches: Why Cyber Incidents Are Costing Businesses a Fortune, Role of CMA in Cyber Security, Forensic Accounting, Fraud Detection, and the Evolving Role of CMAs in Value Protection, Digital Forensic Auditing: Combating Cyber and Financial Crimes, Cyber Risk Costing and Risk Governance, and many more. The contributions collectively highlight the expanding strategic role of CMAs in safeguarding organizational integrity, strengthening internal controls, and driving value protection in the digital age.

The theme for this month's bulletin—"Cybersecurity, Forensic Audit & Digital Vigilance" - is both timely and imperative. As businesses accelerate their digital transformation journeys, the risks they face are no longer confined to traditional financial irregularities. Today, threats are borderless, data-driven, and often invisible until damage is done. Cyber incidents are not merely IT concerns—they are strategic risks with significant financial, reputational, and operational consequences.

I am also delighted to share the grand success of the Students' Regional Cost Convention (SRCC) 2026, held on 17th & 18th March 2026 at Platinum Hall, SIECC Auditorium, Surat, hosted by the ICMAI Surat Chapter. The inauguration ceremony was graced by eminent dignitaries including Shri Hardik Kothiya, Chairman & Joint Managing Director, Rayson Solar Ltd, as Chief Guest, Shri Nikhil Madrasi, President, SGCCI, as Guest of Honour, along with the CMA TCA Srinivasa Prasad, President ICMAI, CMA Neeraj D Joshi, Vice President - ICMAI, CMA (Dr.) Dhananjay V Joshi, Former President – ICMAI and my esteemed council colleagues. With participation from over 800 enthusiastic CMA students, the convention was a vibrant blend of knowledge, competition, and cultural celebration - truly reflecting resounding success and a celebration of knowledge, talent, and professional spirit.

Further, WIRC of ICMAI is organizing "मंथन – 3rd Regional Tax Conclave 2026" on 26th April 2026 at Bhilai. The theme, "Strengthening Economic Growth through Tax Reforms and Compliances," is both timely and significant. I encourage all members to actively participate and benefit from the deliberations.

I extend my sincere gratitude to all the contributors for their valuable articles and unwavering support in enriching this Bulletin. Your insights and efforts continue to make this publication a meaningful platform for knowledge sharing and professional development.

The theme for the May 2026 issue of the WIRC Bulletin is "Cost Audit Excellence: Peer Review and Evolving Practices." I warmly invite members and students to contribute their articles and share their perspectives. Your feedback and suggestions are always welcome and will help us further enhance the quality and relevance of the Bulletin.

As we move forward in this new financial year, let us embrace change, strengthen our competencies, and uphold the highest standards of professionalism.
"In a digital world driven by data, vigilance is not optional - it is the foundation of trust."

Regards,
CMA Nanty Nalinkumar Shah
Vice Chairman &
Chairman Editorial Board –WIRC Bulletin
ICMAI-WIRC

Written by,

CMA Arjya Priya Sinha

Mob - 8918860947

Email - cmaarjyapriyasinha13@gmail.com

Data Breaches: Why Cyber Incidents Are Costing Businesses a Fortune

Imagine logging into your company's systems one morning, only to find hackers have made off with customer data, intellectual property, and your financial records. The immediate panic is bad enough—but the real sting comes later, in the form of multimillion-dollar bills that linger for years. Data breaches aren't just IT headaches; they're financial disasters that can cripple even the mightiest corporations.[1][2]

In this article, we'll dive into the escalating costs of data breaches, unpack the components that drive these expenses, explore real-world examples, and outline strategies to mitigate the damage. Drawing from the latest 2025 reports, we'll reveal why the global average breach now hits $4.4 million—and why it's climbing in key regions like the US at $10.22 million.[2][3][1]

The Alarming Rise in Breach Costs

Data breach expenses have surged over the past decade, outpacing inflation and turning cybersecurity into a boardroom priority. The IBM Cost of a Data Breach Report 2025 pegs the global average at $4.4 million, a slight dip from 2024's record $4.88 million but still 10% higher than pre-pandemic levels. This figure represents direct costs like forensics and fines, plus indirect hits such as lost business.[3][1][2]

In the US, costs soared to $10.22 million per incident, driven by stricter regulations and higher detection expenses. Healthcare leads the pack at $7.42 million per breach, followed by finance ($5.56 million) and tech ($4.79 million), where sensitive data amplifies the fallout. Slower response times exacerbate this: breaches taking over 200 days to contain average $5.01 million, versus quicker ones.[1][2]

These trends signal a perfect storm—ransomware proliferation, AI-powered attacks, and regulatory scrutiny are inflating bills faster than ever.[4][5]

Breaking Down the Cost Components

A data breach's price tag isn't a single line item; it's a cascade of expenses across detection, response, and recovery. Here's a closer look at the biggest drivers, based on 2025 data.

Direct Financial Hits

- **Notification and Compliance:** Companies must alert affected customers and regulators, often under laws like GDPR or CCPA. Fines can reach 4% of global revenue under GDPR, with US breaches facing SEC disclosure mandates.[5]
- **Forensic Investigation:** Hiring experts to trace the breach costs millions; lost business from downtime adds operational pain, hitting $88,000 per hour in some sectors.[6]
- **Ransom and Remediation:** Ransomware victims pay up front, but recovery tech and staffing push totals higher.[5]

Hidden and Long-Term Costs

Post-breach response, including customer service desks, accounts for a huge chunk—up to 51% of costs hit in year one. Customer churn erodes revenue: breached firms lose 20-30% of clients on average. Reputational damage lingers, slashing stock prices by 7-15% and stalling growth.[2][6]

Per-record costs average $160 globally in 2025, down slightly but devastating for large-scale leaks. For context, the 2021 Colonial Pipeline ransomware attack cost $4.4 million directly, but supply disruptions spiked fuel prices nationwide, amplifying economic ripple effects.[7][2]

Cost Category	Global Average (2025)	US Average (2025)	Key Driver [1][2]
Detection & Escalation	$1.58M	$3.5M	Extended timelines
Notification	$0.52M	$1.2M	Regulatory fines
Lost Business	$1.42M	$3.1M	Customer loss/downtime
Post-Breach Response	$1.88M	$2.5M	Help desks, PR

This table illustrates how US firms bear 2-3x the global burden, underscoring geographic risk.[1]

Industry-Specific Nightmares

No sector escapes unscathed, but some feel the burn more acutely. Healthcare's $7.42 million average stems from HIPAA penalties and patient trust erosion—think the 2023 Change Healthcare breach disrupting US prescriptions for weeks.[1]

Finance faces $5.56 million hits from fraud spikes post-breach; retail, at $3.54 million, suffers inventory chaos and boycotts. Even education ($3.8 million) grapples with intellectual property theft. Smaller businesses fare worse proportionally, often folding after a single incident due to limited reserves.[6][1]

Globally, the Middle East clocks $7.29 million averages, while Japan sees $3.65 million—regional laws and attack sophistication dictate variance.[2]

Case Studies: Lessons from the Trenches

Real breaches drive the stats home. Equifax's 2017 leak exposed 147 million records, costing $1.4 billion in settlements, fines, and upgrades—far beyond initial estimates. More recently, the 2024 MOVEit supply chain attack hit thousands of firms, with per-victim costs exceeding $10 million amid cascading notifications.[8][4]

In India, the 2023 Air India breach leaked 4.5 million passengers' data, triggering regulatory probes and a reputational hit amid rising cyber threats in Asia. These stories show breaches evolve: from phishing to sophisticated supply-chain exploits, costs compound with scale.[9][3]

The Human and Strategic Toll

Beyond dollars, breaches erode morale—employees burn out on 24/7 response, and executives face lawsuits. Strategically, firms lose competitive edge: innovation stalls as budgets shift to recovery. Customers vote with their feet, with 57% switching providers after a breach.[3][6]

For CMAs like you, this translates to valuation hits—breached firms trade at discounts, complicating audits and investor pitches. ESG scores plummet too, alienating sustainability-focused stakeholders.

Mitigating the Madness: Proactive Defense

The good news? Prevention slashes costs by 50% for fast responders. Key steps include:[2]

- **Zero-Trust Architecture:** Verify every access, curbing insider threats.
- **AI-Driven Monitoring:** Spot anomalies in under 200 days to cap expenses.[2]
- **Incident Response Plans:** Regular drills cut detection time by 100 days.[1]
- **Cyber Insurance:** Covers gaps, though premiums rise 20% post-breach.[5]
- **Employee Training:** Phishing simulations reduce human-error incidents by 70%.[3]

Investing $1 in prevention saves $7 in cure, per IBM—prioritize cloud security and multi-factor authentication.[4]

Future Outlook: Bracing for More Pain

By 2026, costs could hit $5 million globally as quantum threats and deepfakes emerge. Regulations like India's DPDP Act will mirror GDPR, hiking fines for non-compliance. Businesses must embed cyber resilience in strategy, treating breaches as inevitable but containable.[3]

For finance pros, quantify risks in valuations: factor breach probabilities into discounted cash flows. Tools like IBM's calculator help model scenarios.[1]

In closing, data breaches are the unseen taxes of the digital age—relentless, rising, and ruinous. But armed with data and defense, you can shield your operations. Stay vigilant; the next click could cost millions.

References

1) Huntress: Average Cost of a Data Breach 2025[1]
2) Morgan Lewis: Cost of Data Breaches 2024[4]
3) Baldwin: Business Impact of Data Breaches[5]
4) Sealpath: Quantifying Data Breach Costs[7]
5) Varonis: Data Breach Statistics 2025[2]
6) LinkedIn: Rising Costs Insights[9]
7) Magna5: Real Impacts of Breaches[6]
8) ISACA: True Cost of a Data Breach[8]
9) Secureframe: Breach Stats 2026[3]
10) Statista: Global Breach Costs 2024[10]

Call for Articles ---- WIRC BULLETIN --- May 2026 Edition

Theme for May 2026 WIRC Bulletin is Cost Audit Excellence: Peer Review and Evolving

Standards Focus Area

- **Application of Cost Accounting Standards (CAS),**
- **Practical case studies in peer review,**
- **Compliance quality,**
- **Professional ethics in cost audits.**

Word Limit - 2000 words
Submission Deadline: 25th April 2026
Email: wirc@icmai.in
(Subject Line: Articles for - WIRC BULLETIN May 2026 Edition

Written by,

CMA Rajesh Kapadia

Mob - 99090 29382
Email - rajeshanita2007@yahoo.com

Role of CMA in Cyber Security

Introduction

In the modern digital economy, organizations rely heavily on information systems, online transactions, cloud computing, and digital financial platforms. While these technologies improve efficiency and productivity, they also expose organizations to significant cyber risks such as hacking, data breaches, ransomware attacks, and financial fraud.

As a result, cyber security has become a critical aspect of organizational governance and risk management. In this context, the role of a **Cost and Management Accountant (CMA)** has expanded beyond traditional accounting and financial management to include responsibilities related to cyber security, data protection, and financial risk management.

A CMA is a professional responsible for cost management, financial planning, internal control, performance evaluation, and strategic decision-making within an organization.

Since most cyber attacks target financial systems, payment platforms, and confidential business data, CMAs play an important role in identifying cyber risks, strengthening internal controls, preventing financial fraud, and ensuring compliance with regulatory requirements.

By combining financial expertise with risk management practices, CMAs contribute significantly to the development of a secure and resilient digital business environment.

The various roles played by CMAs in cyber security, including cyber risk management, internal control design, cyber fraud detection, cyber security budgeting, regulatory compliance, and business continuity planning are explained here under

1. Cyber Risk Management

One of the most important roles of a CMA in cyber security is cyber risk management. Cyber risks refer to the potential threats that can affect an organization's information systems, financial databases, and digital assets. These risks include hacking, malware attacks, phishing scams, ransomware attacks, and unauthorized access to financial data.

CMAs help organizations identify and assess cyber risks that may affect financial operations. They analyze vulnerabilities in accounting systems, enterprise resource planning (ERP) software, and digital payment systems.

By evaluating the potential financial impact of cyber attacks, CMAs help management develop strategies to minimize risks.

For example, if a company uses an online payment gateway, a CMA may assess the risk of unauthorized transactions or data breaches.

Based on this assessment, the CMA may recommend stronger authentication methods, encryption technologies, and regular monitoring of financial transactions.

Thus, CMAs play a key role in integrating cyber risk management into the overall risk management framework of the organization.

2. Designing and Strengthening Internal Controls

Internal controls are procedures and policies designed to safeguard assets, ensure accurate financial reporting, and prevent fraud.

In the digital age, internal controls must also address cyber threats and data security issues.

CMAs are responsible for designing and implementing strong internal control systems that protect financial data from cyber attacks.

They ensure that only authorized personnel have access to financial systems and that sensitive data is protected from unauthorized modification or deletion.

Some examples of cyber-related internal controls which CMAs can implement include:

- **Access control mechanisms for accounting software and financial databases**

There are different levels of access like entry, edit, approving, sanction, viewing the reports, processing the reports etc and the user will have to mention specific rights required for his / her function with due concurrence of Head of the Department
Request for new developments or modification in the program, form, report, view etc will be initiated by the user which shall be duly concurred by the concerned Head of the Department and thereafter will get forwarded to IT Department.
IT department will review, revise, reject, approve the request after assessing operational, technical or economic feasibility.
This request shall be submitted online and status of the same shall be available to users online.

- **Segregation of duties in digital financial transactions**

Segregation of duties with respect to entry, edit, approve, processing the reports, editing the reports, approving the reports, viewing the reports etc

- **Password policies and multi-factor authentication systems**

It is recommended to change the password time to time to maintain confidentiality
Not to share passwords with anyone, including assistants, supervisors or co-workers
Not to reveal password over the phone line, in email messages, in any questionnaires

- **Regular monitoring of system logs and transaction records**

Often CMAs advise Information Technology Head to take history of System Logs and Transactions Records from ERP System to ensure that it contains the login id of only authorised executives / officers who are defined in the ERP system to safeguard against any malafide data manipulation

- **Secure backup procedures**

Employees shall take regular backups of the business data residing in their decktop, laptop and any other devises.
Additionally, employees must prioritize the back up of critical and sensitive data.
The back up shall be taken only on assets which are owned by the organisation.
The HODs of the respective department has to ensure that the all concerned employees have taken back up of data residing in their decktop and or laptop .
It also needs to be ensured that when any employee is leaving the company, all necessary data is taken from him/her

By strengthening internal controls, CMAs help reduce the risk of cyber fraud, data manipulation, and unauthorized access to financial information.

Whereas MCA stands for Ministry of Corporate Affairs, it also stands for Maker, Checker and Approval / Authorised.

So this MCA should be inbuilt in all important functions like HR, Purchase, Production, Finannce, Marketing, Company Secretary, Information Technology etc across supply chain

Employees shall disclose and divulge data only with authorised personnel and in line with the procedures laid down by the organisation.

Internal controls aim at safeguarding business interest of the company by preventing occurrence of inappropriate, unethical or unlawful behaviour of any users and preventing threats to IT System.

Internal Control should aim at cyber security risks mitigation.

3. Detection and Prevention of Cyber Fraud

Cyber fraud has become a major concern for businesses worldwide. Fraudsters often use sophisticated cyber techniques such as phishing emails, identity theft, fake payment instructions, and malware attacks to steal money or manipulate financial records.

CMAs play an important role in detecting and preventing such fraud.

Their expertise in financial analysis enables them to identify unusual patterns in financial transactions that may indicate cyber fraud.

For instance, a CMA may notice suspicious payments made to unknown vendors or unusual changes in financial data.

By investigating these anomalies, CMAs can detect potential cyber fraud and take corrective actions.

Additionally, CMAs help implement fraud prevention mechanisms such as:

- Transaction monitoring systems
- Vendor verification procedures
- Digital authorization protocols
- Continuous auditing and financial analysis

Through these measures, CMAs help protect organizations from financial losses caused by cyber fraud.

Company should have proper whistle Blowing Policy

This is because most of the frauds are not discovered by either Internal Auditors or by External Auditors but by Whistle Blowing by current employees or previous employees

CMAs should take up with all executives along with Information Technology executive that Password Protocols should never be either compromised or diluted.

4. Budgeting and Cost Management for Cyber Security

Cyber security requires significant financial investment in technology, infrastructure, software, and training.

Organizations must allocate adequate resources to protect their digital systems from cyber threats.

CMAs play a vital role in budgeting and cost management related to cyber security.

They analyze the costs and benefits of various cyber security solutions and help management make informed investment decisions.

For example, a CMA may evaluate the cost of implementing advanced firewall systems, intrusion detection systems, or data encryption technologies.

They assess whether these investments are financially feasible and whether they provide sufficient protection against cyber threats.

By performing cost-benefit analysis, CMAs ensure that cyber security investments are both effective and economically justified. This helps organizations maintain a balance between security and cost efficiency.

5. Compliance with Cyber Security Regulations

Governments and regulatory bodies have introduced several laws and standards to protect digital data and ensure cyber security. Organizations must comply with these regulations to avoid theft of data, manipulation of data and reputational damage.

CMAs play a crucial role in ensuring compliance with cyber security laws and standards. They help organizations develop policies and procedures that align with applicable cyber security laws.

By ensuring compliance with cyber security regulations, CMAs help organizations avoid legal risks and maintain stakeholder confidence.

6. Promoting Cyber Security Awareness

Human error is one of the major causes of cyber security breaches. Employees who are unaware of cyber threats may accidentally click on malicious links, share sensitive information, or use weak passwords.

CMAs help promote cyber security awareness within organizations by encouraging training programs and awareness campaigns. They may work with IT departments to educate employees about cyber risks, safe digital practices, and fraud prevention techniques.

Examples of cyber security awareness initiatives include:

- Training programs on phishing detection
- Workshops on safe data handling practices
- Awareness campaigns on password security
- Guidelines for secure online financial transactions

These initiatives help create a culture of cyber security within the organization.

Required training sessions for promoting cyber security awareness shall be organised for the employees and third party users.

All the records related to training imparted will be duly maintained.

Conclusion

The rapid growth of digital technologies has transformed the way organizations conduct business. However, this digital transformation has also increased the risk of cyber attacks and financial fraud. In this environment, the role of a **Cost and Management Accountant (CMA)** has evolved significantly.

CMAs are no longer limited to traditional accounting functions. They now play a vital role in cyber security by managing cyber risks, designing internal controls, preventing cyber fraud, budgeting for security investments, ensuring regulatory compliance, and planning business continuity strategies.

By combining financial expertise with risk management and strategic planning, CMAs help organizations protect their financial assets and maintain the integrity of their digital systems. As cyber threats continue to grow in complexity, the involvement of CMAs in cyber security will become even more important in ensuring the financial stability and long-term success of organizations.

Therefore, the role of CMAs in cyber security is essential for building a secure, transparent, and resilient digital economy.

Cyber Security Compliance & Awareness

CMAs play a vital role in ensuring organizations comply with cyber security regulations by developing effective policies and procedures. They also promote awareness through training programs, workshops, and campaigns, helping employees understand cyber risks, prevent data breaches, and adopt safe digital practices, thereby strengthening overall security and stakeholder confidence.

Written by,

CMA Suman Datta

Mob - 9004799456

Email - s_datta1968@rediffmail.com

Cybersecurity, Forensic Audit and Digital Vigilance

The accelerating digitization has significantly elevated cyber risk exposure across industries, particularly for Financial Institutions, transforming cybersecurity from a peripheral IT concern into a central governance and financial risk issue. This paper examines the evolving role of Cost and Management Accountant (CMA) as a strategic architect of digital integrity, with a focus on strengthening risk governance frameworks, enhancing cyber resilience, quantifying data breach costs and enabling robust fraud prevention mechanisms. By integrating financial analytics, digital forensic techniques and risk governance frameworks, CMAs bridge the critical gap between technological vulnerabilities and economic consequences. The study underscores the relevance of globally accepted frameworks such as COSO ERM (Committee of Sponsoring Organizations) and NIST (National Institute of Standards and Technology), while contextualizing their application within the regulatory architecture of the Indian financial system. Although the primary emphasis is on banks and NBFCs, the insights extend to the broader economy, where digital trust is increasingly synonymous with financial stability, institutional credibility, and sustainable growth.

1. Introduction

The contemporary financial landscape presents a compelling paradox—unprecedented efficiency coexisting with heightened vulnerability. As India advances toward a digitally empowered economy, with ambitions aligned to a 'Digital FY27' vision, the rapid digitization of banks and NBFCs has significantly outpaced the evolution of traditional control frameworks. Cyber threats have transitioned from hypothetical contingencies to inevitable operational realities.

Recent data indicating that the RBI reportedly thwarted over 61 million cyberattack attempts in a single quarter of 2025 underscores the scale and intensity of this threat environment. For financial institutions, cyber incidents are no longer isolated technological disruptions; they represent material risk events with direct consequences for capital adequacy, liquidity management, reputational capital and regulatory compliance.

In this evolving context, role of CMAs is constantly evolving. No longer confined to cost control and financial reporting, CMA now operates as a strategic enabler of risk governance. While IT specialists focus on system architecture and threat mitigation, CMA provides a critical financial lens—evaluating economic implications of cyber risks and ensuring that digital vigilance is both operationally effective and financially sustainable.

This paper positions CMA at the convergence of cybersecurity, forensic auditing and digital vigilance, emphasizing their role in quantifying risk exposure, strengthening internal control systems and safeguarding institutional integrity within banks and NBFCs, while also contributing to broader economic resilience.

2. Risk Governance Frameworks

CMAs as Architects of Structured Digital Trust

Risk governance within financial institutions often suffers from fragmentation, with cyber risk treated in isolation from financial and operational risk domains. This siloed approach undermines the effectiveness of enterprise-wide risk management. CMA plays a pivotal role in bridging these divides by applying a unified, cost-centric perspective to governance structures.

Frameworks such as COBIT (Control Objectives for Information and Related Technologies), COSO ERM, and NIST Cybersecurity Framework provide robust structural guidance; however, their effectiveness depends on contextual implementation. Within the ambit of RBI's cybersecurity and IT governance guidelines, CMAs ensure that these frameworks are not reduced to compliance checklists but are operationalized as dynamic, financially grounded systems.

A key contribution of CMA lies in translating qualitative risk constructs into **quantitative financial benchmarks**, thereby enabling institutions to define and operationalize their risk appetite with precision. By integrating **Enterprise Risk Management (ERM)** with cost-control principles, CMAs help institutions prioritize capital allocation toward the most critical 'Crown Jewel' assets, ensuring that governance is agile, audited and aligned with organizational goals.

2.1 Framework Integration

Financial institutions rely on a combination of globally recognized and regulator-mandated frameworks, including:

- COSO Enterprise Risk Management (ERM).
- NIST Cybersecurity Framework.
- ISO 31000 Risk Management Standards.
- RBI Cyber Security Framework for Banks and IT guidelines for NBFCs.

From a CMA's standpoint, the integration of these frameworks must facilitate:

- Quantification of cyber risk exposure in financial terms.
- Alignment of risk appetite with capital allocation strategies.
- Seamless integration of IT controls with financial reporting and internal control systems.

2.2 Governance Challenges in Banks and NBFCs

Banks and NBFCs operate within a uniquely complex risk environment characterized by:

- Extensive reliance on third-party vendors and fintech partnerships.
- Rising instances of digital lending and identity-based frauds.
- Legacy infrastructure vulnerabilities in traditional banking systems.
- Heightened regulatory expectations around operational resilience.

The governance lapses observed in IL&FS crisis (2018) and Yes Bank (2020) illustrate how fragmented risk frameworks and weak oversight can escalate into systemic failures, reinforcing need for integrated, CMA-driven enterprise risk governance models.

CMAs perform RCAs to address these challenges by embedding **risk-adjusted performance metrics** and **build control frameworks** to prevent recurrences and safeguard cybersecurity investments are directly linked to enterprise value protection and long-term sustainability.

3. Cyber Resilience Strategies

From Compliance to Continuity

Cybersecurity, in its traditional sense, emphasizes prevention; cyber resilience, however, focuses on survival and continuity in the face of inevitable breaches. For banks and NBFCs, where even short-duration disruptions can trigger liquidity stress and reputational damage, resilience is a strategic necessity.

The repeated digital outages at HDFC Bank (2020–2022) led to regulatory restrictions by RBI, underscores the financial and reputational costs of inadequate resilience planning, highlighting the need for sustained investment in robust IT infrastructure and business continuity frameworks.

3.1 Key Pillars in Financial Sector Context

- **Preventive Controls:** Multi-factor authentication, encryption, zero-trust architecture
- **Detective Controls:** Security Operations Centres (SOC), SIEM-based monitoring
- **Responsive Mechanisms:** Incident response protocols, regulatory reporting (CERT-In, RBI)
- **Recovery Systems:** Disaster Recovery (DR) infrastructure and Business Continuity Planning (BCP)

3.2 CMA's Strategic Contribution

CMAs enhance cyber resilience through:

- Cost optimization of cybersecurity investments
- Scenario-based financial modeling of cyber incidents
- Capital budgeting for resilience infrastructure
- Financial evaluation of vendor dependencies and contractual safeguards

Importantly, CMAs extend the concept of recovery beyond technical metrics such as Recovery Time Objectives (RTOs) to **Economic Recovery Thresholds**, ensuring that resilience strategies are aligned with financial viability. By evaluating trade-off between redundancy costs and potential failure losses, CMAs facilitate the development of financially optimized, fail-safe architectures.

4. The Anatomy of Data Breach Costing

Valuing the Invisible: The CMA's Precision Lens

The true cost of a cyber incident extends far beyond immediate remediation expenses. For financial institutions, where trust is the core asset, the implications of data breaches are both direct and systemic. A CMA's expertise is crucial in calculating the **Total Cost of Ownership (TCO)** of a cyber incident.

4.1 Components of Data Breach Costs

- **Direct Costs:** Investigation, remediation, legal penalties, regulatory fines and customer notifications.
- **Indirect Costs:** Customer attrition, reputational damage, productivity loss, increased insurance premiums and management bandwidth diversion.
- **Systemic Costs:** Brand erosion, market confidence decline and contagion effects within financial system.

4.2 Relevance for Banks and NBFCs

Data breaches in financial institutions can lead to:

- Loss of depositor and investor confidence.
- Liquidity pressures and funding challenges.
- Increased cost of capital.
- Stringent regulatory interventions.

The Cosmos Bank cyberattack (2018), involving losses of over ₹90 crore through ATM and SWIFT channel compromises, demonstrates the multi-layered cost implications of cyber incidents, including cross-border fraud exposure and recovery complexities.

4.3 CMA-Led Costing Models

CMAs employ advanced costing methodologies to quantify cyber risk, including:

- Activity-Based Costing (ABC) for granular cost allocation
- Lifecycle costing across detection, containment and recovery phases
- Monte Carlo simulations for probabilistic risk estimation

Such models enable boards and senior management to understand the **true economic impact of cyber incidents**, thereby strengthening decision-making and provisioning strategies.

5. Digital Forensic Techniques in Financial Fraud Detection

From Paper Trails to Packet Trails

Digital forensics has redefined the investigative landscape, particularly in the context of financial fraud. It involves the systematic identification, preservation, and analysis of electronic evidence to reconstruct fraudulent activities.

5.1 Key Techniques

- Transaction forensics for fund flow analysis.
- Log and access analysis for detecting unauthorized activities.
- Email and communication forensics for phishing detection.
- Device and disk analysis for data recovery.

5.2 Application in Banks and NBFCs

- Detection of loan origination frauds
- Identification of synthetic identities in digital lending
- Investigation of insider collusion
- Analysis of UPI and card-based fraud patterns

The PMC Bank fraud (2019), involving systematic manipulation of core banking data and concealment of NPAs through dummy accounts, highlights the critical role of digital forensics in uncovering structured financial misreporting and ensuring data integrity.

5.3 CMA's Role

CMAs integrate financial analytics with forensic methodologies, applying professional scepticism and data-driven tools such as Benford's Law, ratio analysis, and trend analytics. Their role extends to:

- Establishing fraud patterns
- Quantifying financial impact
- Supporting legal proceedings under frameworks such as IBC and SARFAESI
- Strengthening audit defensibility

6. Digital Vigilance and Continuous Monitoring

An 'Always-On' Assurance Framework

Digital vigilance and continuous monitoring are proactive cybersecurity and operational strategies involving the ongoing, automated and real-time observation of an organization's digital infrastructure to detect and mitigate risks, threats and compliance breaches instantly. This represents a paradigm shift from reactive, periodic audits (like annual check-ups) to an 'always-on' approach that keeps pace with evolving cyber threats.

6.1 Key Components

- Real-time transaction monitoring systems.
- AI-driven anomaly detection.
- Continuous auditing platforms.
- User behavior analytics.

6.2 Financial Sector Imperatives

- High transaction volumes necessitating automation.
- Need for near real-time fraud detection.
- Regulatory mandates for continuous oversight.

The Union Bank of India SWIFT fraud (2016), triggered by a phishing attack and inadequate real-time monitoring controls, illustrates the necessity of continuous transaction surveillance and automated anomaly detection mechanisms in financial institutions.

6.3 CMA's Contribution

CMAs ensure that digital vigilance systems are:

- Economically viable and scalable.
- Integrated with financial control frameworks.
- Measurable in terms of return on investment.

This transforms internal audit into a continuous assurance function, enhancing both efficiency and effectiveness.

7. CMA in Fraud Prevention: From Control to Culture

Fraud prevention requires a combination of robust systems and ethical governance. The most cost-effective way to manage fraud is to prevent it. In the Indian banking context, where NPAs are often linked to wilful defaults and fraudulent diversions, the CMA's role in monitoring Early Warning Signals (EWS) is paramount.

7.1 Key Areas of Intervention

- Internal control design (segregation of duties, maker-checker mechanisms)
- Predictive analytics for fraud detection
- Whistleblower mechanisms
- Policy formulation and compliance oversight

The proliferation of digital lending app frauds across the NBFC ecosystem (2021–2024) has exposed gaps in vendor due diligence, data governance and regulatory compliance, reinforcing the importance of CMA-led control frameworks and early warning systems.

7.2 Advanced Analytical Tools

- Benford's Law for anomaly detection
- Machine learning-based algorithms for fraud prediction and detection
- Management Control Systems (MCS)

7.3 Strategic Impact

CMAs contribute to:

- Reduction in fraud losses
- Enhanced regulatory compliance
- Strengthened stakeholder confidence

By embedding Internal Controls over Financial Reporting (ICFR) within digital systems and leveraging variance analysis and budgetary controls, CMAs enable transition from reactive detection to predictive prevention. They create a transparent environment where deviations can be predicted and flagged in real-time and aid to transform the organization from a 'detect and react' posture to a 'predict and prevent' stance, ensuring that it remains a going concern.

8. Broader Economic Implications

Cybersecurity failures within financial institutions can trigger systemic consequences, including financial instability, disruption of payment systems, erosion of investor confidence and macroeconomic shocks. A secure and resilient financial sector is therefore indispensable for sustaining economic growth, financial inclusion and global competitiveness.

And this is not limited to financial sector viz. the ransomware attack on AIIMS Delhi (2022), demonstrated how cyber incidents can disrupt critical infrastructure at scale, offering a parallel to the potential systemic risks posed to banking and payment ecosystems.

9. Conclusion

Cybersecurity, forensic auditing and digital vigilance have emerged as integral components of financial governance. For banks and NBFCs, these dimensions are critical to maintaining stability, trust, and regulatory compliance.

Some of the real-world incidents from the Indian ecosystem reinforce that cyber risk is not merely a technological concern but a strategic financial risk requiring structured oversight, quantitative evaluation and proactive governance by CMAs.

CMAs stand at the forefront of this transformation—bridging the gap between technological risk and financial impact. By embedding structured risk governance frameworks, driving cyber resilience, quantifying data breach costs and leveraging forensic analytics, CMAs play a pivotal role in building institutions that are secure, resilient and future-ready.

References

- Reserve Bank of India (RBI). (2016). Cyber Security Framework in Banks.
- RBI. Master Directions on IT Framework for NBFCs.
- National Institute of Standards and Technology (NIST). Cybersecurity Framework.
- Committee of Sponsoring Organizations (COSO). Enterprise Risk Management Framework.
- ISO. (2018). ISO 31000: Risk Management Guidelines.
- IBM Security. (2023). Cost of a Data Breach Report.
- CERT-In. Guidelines on Cyber Incident Reporting.
- PwC. (2022). Global Economic Crime and Fraud Survey.
- ACFE. (2023). Report to the Nations on Occupational Fraud and Abuse.
- ISACA. COBIT Framework for IT Governance.

Written by,
CMA Pradnya Y. Chandorkar
Mob - 99228 67455
Email - chandorkar.pradnya@gmail.com

Written by,
Srivathsa K,
Mob - 94452 95795
Email - srivathsakumar2001@gmail.com

Forensic Accounting, Fraud Detection, and the Evolving Role of Cost and Management Accountants(CMA's) in Value Protection

Abstract

Forensic accounting has evolved from a niche investigative service into a core capability for organizations seeking to protect value in an environment shaped by digital payments, complex financing structures, and rapidly evolving fraud typologies. This article revisits the role of Cost and Management Accountants (CMAs) through a source-verified review of global and Indian evidence. It highlights how CMAs, through their expertise in cost structures, operational processes, and analytical tools, are uniquely positioned to contribute to fraud detection, financial forensics, and value protection.

Background

Forensic accounting and financial forensics involve the application of accounting skills to investigate financial misconduct such as fraud, embezzlement, and money laundering and to provide evidence in legal contexts. Unlike routine auditing, which focuses on the accuracy of financial statements, forensic accounting is investigative and often litigation oriented. Its importance has grown with globalization and digitization.

Recent data underscore the scale of financial crime. A global study by the Association of Certified Fraud Examiners (ACFE, 2024) estimates that organizations lose approximately 5% of their annual revenues to occupational fraud. In India, the rapid expansion of digital banking has been accompanied by high-profile fraud cases, further emphasizing the need for robust forensic capabilities.

Recent regulatory and academic developments are also reshaping the field. The Institute of Chartered Accountants of India (ICAI) issued mandatory Forensic Accounting and Investigation Standards (FAIS) in July 2023. The Financial Action Task Force (FATF) continues to update guidance on money laundering (ML) and terrorist financing (TF) risks. These developments call for forensic accountants to be proficient not only in financial analysis but also in digital forensics, legal frameworks, and data analytics.

Why CMAs Add Value

Fraud is no longer limited to isolated acts of embezzlement. It increasingly manifests as a systems-level issue embedded in procurement, lending, revenue recognition, vendor management, and digital payment ecosystems. Consequently, fraud detection cannot rely on a single control layer or a single profession; it requires a combination of accounting judgment, operational insight, legal awareness, and data-driven investigation.

Cost and Management Accountants are strategically positioned in this context. Their work is grounded in reconciling physical flows with financial records material consumption against output, overhead absorption against production patterns, and transactional behaviour against operating reality. These reconciliations are valuable not only for cost control but also for identifying red flags such as unexplained variances, suspicious vendor relationships, abnormal pricing patterns, and repeated exceptions in master data.

In the broader context of organized financial crime, companies can be misused as channels for money laundering (ML) and terrorist financing (TF). CMAs apply tools such as systems analysis, ratio analysis, and financial modelling to identify financial abnormalities, which can serve as early indicators of potential involvement in illegal activities.

The traditional approach to fraud detection has often been reactive focused on after-the-fact identification. In contrast, CMA expertise in standard costing and variance analysis provides a proactive early warning mechanism. Persistent, unexplained unfavourable variances in material usage, for example, may indicate inventory shrinkage or fictitious procurement schemes. Further,

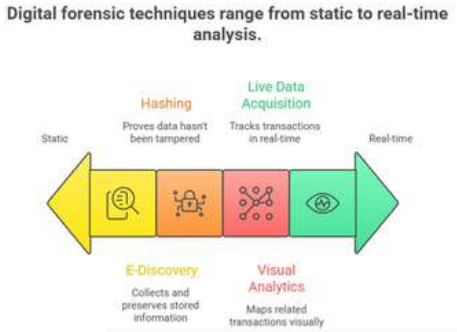
Cost Audit Reports provide detailed operational cost structures, helping connect financial data with underlying activities and uncover potential irregularities.

From Cost Accounting to Financial Forensics

From the CMA perspective, the current environment represents a mandate to act as an architect of organizational integrity. By integrating financial forensic techniques with granular cost analysis, CMAs can identify misclassification of cost heads, overstatement of overheads, and potential collusion among stakeholders.

The evolving approach necessitates a transition from traditional accounting toward financial forensics. While the terms are often used interchangeably, financial forensics is sometimes viewed as a broader, multidisciplinary approach that integrates accounting, digital forensics, investigative due diligence, and legal processes.

The Digital Frontier: Data as Primary Evidence



While physical audit of records remains important, conclusive evidence of corporate fraud is increasingly found in digital footprints across Enterprise Resource Planning (ERP) systems, cloud storage, and communication platforms.

- **Electronic Discovery (E-Discovery) and Metadata Analysis -** Digital forensic procedure begins with E-discovery. This involves systematic identification, collection, and preservation of Electronically Stored Information (ESI). Beyond the content of a document, CMAs now analyse metadata (a set of data that describes and gives information about other data). Metadata can highlight a backdated purchase order, person who modified vendor data in the master file or accessed sensitive cost sheet from an unauthorized IP address outside of office hours.

- **Live Data Acquisition vs. Dead Analysis -** Traditional auditing is more of a dead analysis i.e., analysing financial records pertaining to previous year. Digital forensic procedures allow for live data acquisition, where a CMA monitors the ERP environment in real-time. By utilising log file analysis, CMAs can track every keystroke associated with high-value transactions. If a user attempts to bypass a control, the digital trail provides irrefutable evidence of intent - which is a core component of the Fraud Triangle.

- **Hashing and Data Integrity -** A critical concern in forensic investigations is the admissibility of evidence. By adopting the use of Hash Values (digital fingerprints) and cryptographic hash (such as SHA-256) of a financial database at the start of an investigation, CMAs can prove that the data has not been tampered during the analysis. This ensures that the findings of a Cost or Management Audit can withstand the scrutiny of a court of law or a disciplinary committee.

- **Visual Analytics and Link Analysis -** Digital forensic software allows the investigator to move beyond spreadsheets into link analysis. This technique visually maps Related party Transactions by identifying relationships between entities, bank accounts, and timestamps. For instance, if a company is suspected of Round-Tripping (moving money to a shell company only for it to return as revenue), link analysis software can instantly visualise the circular flow of funds by highlighting nodes that represent shared directors or identical registered addresses, that would be invisible in a standard tabular report. Further, it allows CMAs to transcend from analysing traditional ledgers to uncover hidden circularity in transactions, where funds apparently paid to vendors were routed back to promoters through a web of subsidiary entities.

Digital evidence and analytical methods

Modern investigative environments generate extensive metadata, including timestamps, user IDs, approval trails, device locations, master-data changes, and system exceptions. These elements help reconstruct events and establish accountability regarding who performed specific actions, when, and from where.

Digital evidence must be preserved with a clear chain of custody, and legal admissibility requirements must be strictly followed. Forensic teams therefore require a working understanding of both technology and evidentiary procedures.

Analytical tools such as Benford's Law analysis, link analysis, anomaly detection, and exception reporting enhance the ability to move from sample-based reviews to full-population testing. These tools complement, rather than replace, professional judgment and skepticism.

Combatting Sophisticated Fraud Typologies

As of 2026, fraud typologies have increasingly shifted toward cyber-enabled fraud and trade-based money laundering (TBML). FATF guidance highlights cyber-enabled fraud as one of the most damaging forms of profit-driven crime globally.

Fraudsters often use complex financial structures and shell entities to obscure beneficial ownership. Accountants play a key role in uncovering such structures by tracing fund flows and identifying relationships between entities.

TBML allows illicit profits to be disguised within legitimate trade transactions. Digital forensic techniques can identify inflated invoices, falsified documentation, and fictitious entities used to conceal financial flows.

With the integration of advanced analytics and AI-driven dashboards, professionals can apply techniques such as Benford's Law and Relative Size Factor (RSF) analysis across large datasets in near real time. These tools help detect anomalies such as unusual transaction timing, round-value entries, and vendor patterns that traditional sampling methods may overlook.

System logs and audit trails provide detailed visibility into user actions. Attempts to bypass controls can be identified through these digital traces, which serve as strong evidentiary indicators when combined with contextual analysis.

Electronic Discovery and Real-Time Monitoring

Digital forensic procedures begin with electronic discovery (e-discovery), involving the identification, collection, and preservation of electronically stored information (ESI). Beyond document content, metadata analysis can reveal backdated transactions, unauthorized modifications, and access from unusual locations.

Traditional auditing is largely retrospective ("dead analysis"), focusing on historical data. In contrast, digital forensic approaches enable real-time monitoring ("live data acquisition"), allowing CMAs to observe system activity continuously and detect irregularities as they occur.

Practical Plug Points

- Treat fraud statistics as indicators rather than absolutes; always examine reporting context, timing, and classification.
- Use cost records as an investigative lens; variance analysis and cost allocation patterns can reveal hidden anomalies.
- Preserve digital evidence properly, ensuring chain-of-custody and legal admissibility.
- Promote a speak-up culture; evidence consistently shows that tips are a leading detection mechanism.
- Align forensic work with FAIS and AML/CFT frameworks to ensure defensible and standardized reporting.

Conclusion

As India progresses toward a USD 5 trillion economy and beyond, the role of the CMA is evolving from that of a traditional accountant to a guardian of economic integrity shifting from value recording to value protection.

By mitigating fraud risks, CMAs contribute to reducing risk premiums and enhancing investor confidence, thereby supporting capital efficiency and economic growth. Evidence from ACFE highlights the importance of human reporting mechanisms, while RBI insights on fraud reporting emphasize contextual interpretation.

CMAs are uniquely positioned to bridge financial data and operational realities. Their role is not to replace existing assurance functions but to strengthen them by integrating Cost Intelligence (CI) with forensic analysis.

References

- Association of Certified Fraud Examiners (ACFE). (2024). Occupational Fraud 2024: A Report to the Nations.
- Financial Action Task Force (FATF). (2024). India Mutual Evaluation Report.
- Financial Action Task Force (FATF). (2025). Comprehensive Update on Terrorist Financing Risks.
- Institute of Chartered Accountants of India (ICAI). (2023). Forensic Accounting and Investigation Standards (FAIS).
- Reserve Bank of India (RBI). (2024). Annual Report 2023–24.
- Reserve Bank of India (RBI). (2025). Annual Report 2024–25.

Written by,

CMA Jayesh Dayama

Mob - +91 8446332770

Email - Jayeshdayama26@gmail.com

Cybersecurity, Forensic Audit & Digital Vigilance: A New-Age Shield Against Vendor Fraud

In today's increasingly digitized business environment, organizations rely heavily on vendors for critical operations—procurement, IT services, logistics, and financial processes. While this ecosystem enhances efficiency, it also opens doors to sophisticated fraud schemes. Traditional audit mechanisms alone are no longer sufficient. The convergence of cybersecurity, forensic audit, and digital vigilance has become essential in detecting and preventing vendor-side fraud.

Understanding Vendor Fraud in the Digital Era

Vendor fraud typically involves manipulation, misrepresentation, or collusion by external parties (sometimes in conjunction with internal employees) to siphon off funds or resources. With digital systems in place, fraudsters have evolved their methods.

Common Types of Vendor Fraud

1. **Fake Vendor Creation (Shell Vendors):** Fraudsters create fictitious vendors in the system and raise invoices for non-existent goods/services.
2. **Invoice Manipulation:** Genuine vendors inflate invoices, duplicate billing, or alter payment details (bank account fraud).
3. **Collusion with Employees:** Internal staff may approve fraudulent invoices or bypass controls in exchange for kickbacks.
4. **Phishing & Payment Diversion Fraud:** Cybercriminals impersonate vendors via email and request changes in bank details.
5. **Overbilling & Quantity Fraud:** Vendors charge for higher quantities or superior quality than actually supplied.

Role of Cybersecurity in Preventing Vendor Fraud

Cybersecurity forms the first line of defense by securing systems, communication, and data integrity.

Key Measures:

- Access Control & Segregation of Duties (SoD) : Restrict vendor master changes to authorized personnel only.
- Multi-Factor Authentication (MFA) : Prevent unauthorized system access, especially in ERP systems.
- Email Security & Phishing Detection : Use advanced filters to detect spoofed emails requesting payment changes.
- Audit Trails & Logs : Maintain detailed logs of vendor creation, modification, and payment processing.
- Data Encryption : Protect sensitive vendor and financial data from breaches.

Forensic Audit: Detecting the Invisible

Forensic audit goes beyond routine checks—it investigates anomalies, patterns, and intent behind transactions.

Techniques Used in Vendor Fraud Detection :

- Benford's Law Analysis

Identifies unnatural number patterns in invoices :

- Duplicate Invoice Testing

Detects repeated invoice numbers, amounts, or dates :

- Vendor Master Analysis

Flags vendors with:

- Same bank accounts
- Similar addresses
- Missing GST or compliance details

- Round-Amount Transactions

Unusual frequency of rounded payments can indicate manipulation.

- Timing Analysis

Transactions processed outside business hours or near period-end.

Digital Vigilance: Leveraging Digital Footprints

Every digital action leaves a trace. Digital vigilance focuses on tracking and analyzing these footprints.

Key Indicators from Digital Footprints:

- IP Address Tracking

Multiple vendor accounts accessed from the same IP.

- Device Fingerprinting

Identifying if vendor and employee logins originate from the same device.

- Email Metadata Analysis

Detecting spoofed domains or subtle variations in email IDs.

- Geo-location Analysis

Vendor claiming to be in one country but accessing systems from another.

- User Behavior Analytics (UBA)

Sudden spikes in activity or unusual patterns by employees handling vendor payments.

Case Illustration: Payment Diversion Fraud

A company received an email from a "vendor" requesting a change in bank details. The email looked legitimate, with identical branding and signature.

What Happened?

- The email domain had a minor variation (e.g., .co instead of .com)
- Payment was processed without independent verification
- Funds were transferred to a fraudulent account

How It Could Have Been Prevented:

- Email domain verification through cybersecurity tools
- Maker-checker control for bank detail changes
- Vendor confirmation via registered contact details
- Monitoring of email anomalies through digital vigilance

Integrated Approach: The Way Forward

To effectively combat vendor fraud, organizations must adopt an integrated framework:

1. **Preventive Controls**
   - Strong IT controls and cybersecurity framework
   - Vendor onboarding due diligence
   - Automated validation checks in ERP

2. **Detective Controls**
   - Continuous auditing using data analytics
   - Exception reports and red-flag monitoring
   - Periodic forensic reviews

3. **Corrective Actions**
   - Immediate investigation of anomalies
   - Strengthening internal controls
   - Legal and disciplinary action

Conclusion

The landscape of fraud is rapidly evolving with technology. Vendor fraud, once limited to manual manipulation, now leverages digital vulnerabilities. For finance professionals, especially CMAs, the role is no longer confined to numbers—it extends to understanding systems, digital risks, and forensic techniques.

By integrating cybersecurity, forensic audit, and digital vigilance, organizations can build a robust defense mechanism, ensuring transparency, accountability, and financial integrity in an increasingly complex business environment.

Written by,

Heena P.Matalia

Mob - 8511078826

Email - heena.matalia-afm@msubaroda.ac.in

Fortifying the Value Chain: Digital Vigilance, Forensic Cost Auditing, and Working Capital Resilience – The Evolving Role of CMAs (2026)

"In the digital economy, a breached ledger is a broken promise. CMAs are the new-age sentinels, turning bits and bytes into bastions of corporate integrity."

Introduction: The Convergence of Cost and Cyber-Integrity

In the contemporary digital economy, where cost data is deeply embedded within enterprise systems, the role of Cost and Management Accountants (CMAs) has evolved significantly. The intersection of Section 148 of the Companies Act, 2013 with the Digital Personal Data Protection (DPDP) Act, 2023 has redefined the professional landscape.

The Cost and Management Accountant (CMA) is no longer confined to cost sheets and variance analysis. Instead, the CMA emerges as a "Digital Cost Resilience Architect," ensuring that cost data is not only accurate but also secure, traceable, and tamper-proof. No longer confined to traditional cost audit functions, CMAs are emerging as strategic custodians of digital integrity, ensuring that cost records remain accurate, secure, and compliant within an increasingly complex regulatory environment.

The Regulatory Landscape: Beyond Compliance

The evolution of the Companies (Cost Records and Audit) Rules, 2014, especially after the July 2025 amendment (CRA-2 refinement), has shifted the paradigm from retrospective compliance to real-time assurance.

Key Transformations:

- **Rule 5 & 6 Compliance:**

Cost records now require system integrity, not just arithmetic correctness.

- **IT Act, 2000 (Section 7B):**

Recognizes electronic audit trails as legally valid, placing responsibility on CMAs to ensure ERP security.

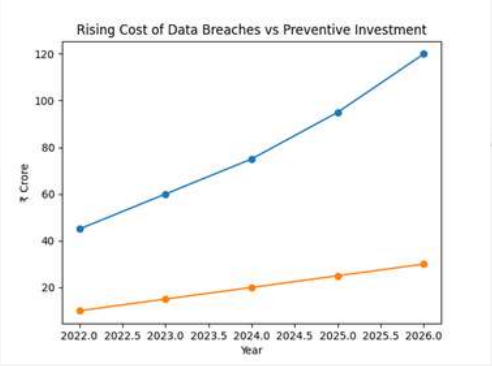
Insight:

A cost statement today is only as reliable as the **digital infrastructure** supporting it.

Section 148 of the Companies Act, 2013, read with the Companies (Cost Records and Audit) Rules, 2014, continues to form the backbone of cost audit in India. However, the transition from manual records to ERP-driven systems has introduced new dimensions of risk. Digital records must now satisfy not only cost accounting standards but also audit trail requirements and cybersecurity controls.

Cybersecurity as a Cost Audit Concern

Cybersecurity is no longer an IT-centric issue; it directly affects cost reliability and financial reporting. Frameworks under the Information Technology Act, 2000 and the Digital Personal Data Protection Act, 2023 require organizations to safeguard financial and operational data. A breach in cost data systems can distort material cost, overheads, and working capital calculations, thereby impacting both statutory compliance and managerial decisions.



The financial implications of cybersecurity failures are substantial. As illustrated in Figure 1, the cost of cyber breaches has shown a steep upward trajectory, significantly outpacing

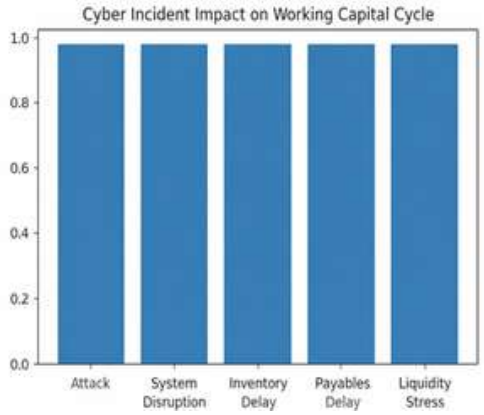
investments in preventive controls. This gap highlights the urgent need for proactive cost-based cybersecurity strategies.

Forensic Audit Integration

Forensic audit techniques are increasingly being integrated into cost audit practices. These include log analysis, anomaly detection, and digital evidence validation. Such techniques enable CMAs to detect manipulated cost allocations, fictitious entries, and irregular patterns that may otherwise go unnoticed in traditional audit approaches.

GST, Working Capital and Technology Linkage

Accurate cost records play a critical role in ensuring GST compliance and optimizing working capital. A disruption in cost systems can lead to incorrect valuation, mismatched input tax credits, and delays in receivables. Figure 2 demonstrates how a cyber incident cascades through the working capital cycle, ultimately affecting liquidity and operational efficiency.



The Triple-Threat Strategy: Technology, GST, and Working Capital

1. **Digital Vigilance: The "Zero-Trust" Costing Model**

In 2026, CMAs adopt a Zero-Trust framework, where:
No data is accepted without validation
Every transaction is **digitally authenticated**

Example:
If a **Material Master** in ERP is altered without dual authorization:
CAS-6 (Material Cost) becomes unreliable
Financial reporting is compromised

Shift in Role:
CMA audits **algorithms and system logic**, not just outputs.

2. **GST Synergies: Forensic ITC Reconciliation**

The linkage between cost audit and GST compliance has become critical.

Key Risk Areas:
Inverted Duty Structures:
AI detects manipulation in cost allocation under CAS-22.

Circular Trading:
Matching GSTR-2B with production capacity (CAS-2) reveals fake transactions.

3. **Working Capital Optimization: The Liquidity Shield**

Cybersecurity and working capital are now interconnected.
A ransomware attack on inventory systems can:

- Freeze operations
- Block liquidity
- Distort cost data

Strategic Role of CMA:

- Use predictive analytics
- Incorporate cyber-risk buffers in inventory planning

Comparative Framework: Traditional vs Digital Forensic Cost Audit

Metric	Traditional Cost Audit	Digital Forensic Cost Audit (2026)
Data Source	Sample-based	100% data population
Verification	Manual checks	Blockchain & hash validation
Focus	Historical	Real-time & predictive
Compliance	Periodic	Continuous monitoring

Illustrative Case Insight

In a recent scenario, a mid-sized manufacturing entity experienced a ransomware attack that distorted its cost data. Through forensic reconstruction, discrepancies in material costs and overhead allocations were identified and corrected. This not only ensured compliance but also helped recover significant working capital, demonstrating the strategic value of integrating cybersecurity with cost audit.

Conclusion

In the evolving digital economy, the role of the Cost and Management Accountant (CMA) has transformed into that of a techno-financial guardian, ensuring not only accuracy in cost determination but also resilience against cyber and data risks. By integrating digital vigilance, forensic analytics, GST reconciliation, and working capital optimization, CMAs contribute significantly to strengthening organizational integrity and sustainability. The convergence of regulatory frameworks, advanced technologies, and cost standards positions CMAs as critical enablers of corporate trust and transparency. Ultimately, digital vigilance is no longer optional but essential, and CMAs stand as the unbreakable link connecting cost integrity with long-term corporate resilience and value creation.

The convergence of cybersecurity, forensic audit, and digital vigilance represents a paradigm shift in the role of CMAs. By embedding these elements into cost audit practices, professionals can enhance reliability, ensure compliance, and create sustainable value in an increasingly digital business environment.

"Digital Vigilance Today, Sustainable Profits Tomorrow:
CMAs – The Unbreakable Link Between Cost Integrity and Corporate Resilience."

References

IBM Security. (2025). Cost of a data breach report (India).

Institute of Cost Accountants of India. (2025). Guidance note on forensic audit.

Ministry of Corporate Affairs. (2025). Cost audit amendment rules.

Sarma, R. (2026). Blockchain and cost auditing. Management Accountant, 61(4), 22–29.

World Economic Forum. (2026). Cyber resilience in supply chains.

Written by,

CMA Shirish Shah

Mob - 9420356025
Email - cmashirish@gmail.com

"Fraud Detection, Prevention & Cure - Powered by CMA." !!!

Abstract

Fraud is rarely accidental-it thrives where systems are weak, costs are misunderstood and vigilance is absent. In this evolving landscape, the Cost and Management Accountant (CMA) emerges not merely as a cost expert but as a strategic defender of financial integrity.

This article challenges the conventional belief that fraud detection is limited to audit-centric roles and positions CMAs at the forefront of prevention and cure. By blending deep cost intelligence with process insight, CMAs are uniquely equipped to identify early warning signals often invisible to others. The discussion spans traditional tools, cutting-edge technologies like AI and analytics and real-world case studies that reveal how overlooked cost distortions often precede major frauds. It ultimately calls upon professionals to rethink their role-not as passive record-keepers but as proactive risk architects-because in the fight against fraud, prevention is power and CMA is precision.

Author Profile

CMA Shirish Shah, FCMA, is an academician with over 40 years of experience. A Fellow of the Institute of Cost & Management Accountants of India and M. Com from Pune University, he has served in senior roles in the corporate sector, academia and university administration. He is a Founder and Mentor at the Commerce Sanskruti Professional Academy and held positions such as Finance Officer at Shivaji University, Director of an MBA institute and nominee on its Senate by Hon Chancellor and Academic Council by Hon. Vice- Chancellor of Shivaji University. He is a regular speaker and contributor on accounting, finance, costing, taxation and management.

Contents of article

In today's complex economic ecosystem, fraud has evolved from simple manipulation to highly sophisticated financial engineering. In such a dynamic environment, the role of a Cost and Management Accountant (CMA) is no longer confined to cost sheets and budgets-it has expanded into becoming a strategic sentinel against fraud.

This article aims to open the eyes of new entrants and professionals alike - "CMA is not just a profession-it is a responsibility towards financial truth."

1. CMA Profession's Prime Objectives -

The CMA profession, guided by the Institute of Cost Accountants of India, is built on three foundational pillars:
Cost Efficiency
Performance Optimization
Strategic Financial Control

But beyond these lies a silent yet critical objective-safeguarding organizational integrity.
A CMA is expected to -
Ensure true and fair cost representation
Detect inefficiencies and leakages
Establish robust internal controls
Provide data-driven decision support
"सत्यमेव जयते" (Truth alone triumphs) - This is not just a national motto but the moral backbone of the CMA profession.

2. Types of Frauds & CMA's Scope of Action

Frauds today span multiple domains. Some key types include -

A. Financial Frauds

#,Revenue manipulation
Expense inflation
Fake invoicing
Inventory misstatements

B. Operational Frauds

Procurement fraud
Payroll fraud
Asset misappropriation

C. Cyber & Digital Frauds

Data manipulation
ERP hacking
Digital payment frauds

D. Regulatory & Compliance Frauds

Tax evasion
GST frauds
Transfer pricing manipulation

Frauds Best Tackled by CMAs

CMAs are especially effective in -

Cost manipulation detection
Inventory frauds
Process inefficiencies leading to leakages
Budgetary deviations
Margin distortions

Why? Because CMAs understand cost behavior, variance and operational flow deeply.
"जहाँ गणना है, वहाँ निगरानी है"
(Where there is calculation, there is control.)

3. Traditional Tools & Techniques for Fraud Control

1. **Variance Analysis**
   Comparing actual vs budget to identify abnormal deviations.

2. **Ratio Analysis**
   Profitability, liquidity and efficiency ratios reveal hidden anomalies.

3. **Standard Costing**
   Helps detect inefficiencies and unusual cost spikes.

4. **Internal Audit Systems**
   Regular checks to ensure compliance and detect irregularities.

5. **Cost Audit**
   A unique domain of CMAs-ensures cost data integrity.

6. **Reconciliation Techniques**
   Bank, inventory and ledger reconciliations uncover discrepancies.

7. **Budgetary Control**
   Tracking financial discipline across departments.
   "Trust, but verify." - A timeless principle of financial control.

4. Advanced Tools & Technologies for Fraud Prevention

Modern fraud requires modern weapons.

1. **Data Analytics & Big Data**
   Analyzing large datasets to detect unusual patterns.

2. **Artificial Intelligence (AI)**
   Predictive fraud detection through behavior analysis.

3. **Blockchain Technology**
   Ensures transparency and immutability in transactions.

4. **ERP Systems with Controls**
   Integrated systems like SAP with audit trails.

5. **Continuous Auditing Tools**
   Real-time fraud monitoring systems.

6. **Forensic Accounting Software**
   Tools for deep financial investigation.

7. **Robotic Process Automation (RPA)**
   Reduces human intervention and fraud scope.

8. **Cybersecurity Systems**
   Protect financial data from digital fraud.
   "योगः कर्मसु कौशलम्"
   (Skill in action is true excellence.)
   A CMA equipped with technology becomes unstoppable in fraud detection.

5. Is Fraud Prevention Only CA's Domain?

Absolutely NOT.

Traditionally, fraud detection has been associated with Chartered Accountants, especially in statutory audits. However -
CMAs bring cost intelligence
CS professionals bring compliance governance
IT experts bring technical controls

Fraud prevention is a multi-disciplinary battlefield.
"It takes a system to create fraud-and a stronger system to prevent it."

6. CMA vs CA vs Others - A Comparative Insight

Fraud detection, prevention, and cure require a coordinated effort among multiple professionals, each bringing a distinct perspective shaped by their training and regulatory role. Here's a concise comparative view:

fChartered Accountants (CAs)

CAs are the frontline defenders in financial integrity. Their primary strength lies in audit, financial reporting and forensic accounting. Through statutory audits, internal audits and tax audits, they detect irregularities such as manipulation of books, revenue inflation or expense suppression. In prevention, they design robust internal controls and ensure compliance with accounting standards. In the "cure" phase, they assist in forensic investigations, quantify fraud impact and support litigation with expert opinions.

Cost & Management Accountants (CMAs)

CMAs focus deeply on cost structures, efficiency and internal financial systems. Their role in fraud detection is more analytical-identifying abnormal cost behavior, variance anomalies and inefficiencies that may indicate fraud (e.g., inflated procurement costs, production leakages). In prevention, they design cost control systems, budgeting frameworks and MIS that reduce scope for manipulation. For cure, CMAs help in restructuring systems, plugging leakages and strengthening operational accountability.

Company Secretaries (CSs)

CS professionals specialize in corporate governance, legal compliance and regulatory frameworks. They detect fraud through compliance checks, secretarial audits and ensuring adherence to company law provisions. Their preventive role is critical-they build governance structures, ensure board discipline, proper disclosuress and ethical conduct. In the cure stage, CSs handle regulatory reporting, coordinate with authorities and ensure corrective legal actions are properly implemented.

Other Professionals

a) Internal Auditors - Continuously monitor systems and transactions, acting as an early warning mechanism for fraud detection and prevention.

b) Forensic Experts - Specialists who investigate complex frauds using digital tools, data analytics and evidence collection techniques.

c) Lawyers/Legal Advisors - Crucial in the cure phase-handling prosecution, recovery and legal enforcement.

d) IT Professionals / Cyber Experts -Detect and prevent digital frauds, strengthen cybersecurity systems and trace electronic evidence.
Bankers & Financial Analysts - Identify suspicious transactions, unusual fund flows and credit-related fraud risks.

In essence,
CAs dominate financial truth verification,
CMAs excel in cost and operational integrity,
CSs ensure governance and legal discipline,
and other professionals provide technical, investigative and enforcement support.

Together, they form a comprehensive ecosystem where fraud can be detected early, prevented systematically and resolved effectively.

7. Unique Edge of CMAs

CMAs possess distinct advantages -
Deep understanding of cost structures
Strong grip on process flows
Expertise in budgetary control
Ability to detect micro-level inefficiencies
Strategic decision-making orientation
“A CMA sees what others overlook.” !!!

8. How CMAs Can Build a Specialized Practice

To capitalize on this field, CMAs should -
Develop expertise in forensic accounting
Learn data analytics tools (Power BI, Python, etc.)
Offer fraud risk assessment services
Conduct internal control reviews
Collaborate with legal & IT experts
Potential Practice Areas
Fraud risk consulting
Cost fraud audits

ERP control audits
Investigation assignments
"Opportunity lies where complexity exists."

9. Role of the CMA Institute

The Institute of Cost Accountants of India must -
Continue Current efforts -
#:Certification courses
Cost audit mandates
Skill development programs
Future Steps to be taken -
Specialized Forensic CMA certification
Industry tie-ups
Advanced tech training
Awareness campaigns
"विद्या ददाति विनयम्"

10. Case Studies - CMA in Action (With Company & Key Details)

A. Domestic Case Studies -

1. Satyam Computer Services
   Nature of Fraud - Inflated revenues, fake cash balances (~₹7,000 crore)
   CMA Relevance - Early signals were visible in cost-revenue mismatches and abnormal margins
   Key Learning - A CMA's cost analysis could have flagged inconsistencies much earlier
   "Numbers don't lie-but manipulated presentation does."

2. Punjab National Bank
   Nature of Fraud - Unauthorized LoUs worth ₹13,000+ crore
   CMA Role Scope - Weak internal controls & reconciliation failures
   Key Learning - Continuous audit & control systems (CMA domain) could have prevented escalation

3. IL&FS
   Nature of Fraud - Debt misreporting, liquidity concealment
   CMA Relevance - Failure in cash flow analysis & cost of capital monitoring
   Key Learning - CMA's expertise in financial planning could have exposed unsustainable structures

4. Kingfisher Airlines
   Nature of Fraud - Fund diversion, loan misuse
   CMA Role - Inefficient cost structures & loss-making operations ignored
   Key Learning- Strong cost control & variance analysis could have flagged early warning signals

5. DHFL
   Nature of Fraud - Loan diversion through shell entities (~₹30,000 crore)
   CMA Relevance - Fund flow tracking & cost audit gaps
   Key Learning - CMA-led forensic cost tracking could detect abnormal lending patterns

6. Yes Bank
   Nature of Fraud - Evergreening of loans, misreporting NPAs
   CMA Role - Weak risk-based costing & asset quality analysis
   Key Learning - CMA's analytical models could have identified stressed asset patterns early

7. National Spot Exchange Limited
   Nature of Fraud - Fake warehouse receipts, commodity trading scam
   CMA Relevance - Lack of inventory verification & cost validation
   Key Learning - CMA expertise in inventory costing could have prevented the fraud

B. International Case Studies

1. Enron Corporation
   Nature of Fraud - Off-balance sheet liabilities, profit manipulation
   CMA Relevance - Hidden cost structures and inflated profitability
   Key Learning - Cost transparency is critical-CMA tools could have exposed distortions

2. WorldCom
   Nature of Fraud - Capitalization of operating expenses (~$11 billion)
   CMA Role - Misclassification of costs
   Key Learning - Strong cost classification systems (CMA domain) could detect such fraud

3. Toshiba
   Nature of Fraud - Profit overstatement due to cost pressure
   CMA Relevance - Unrealistic cost targets leading to manipulation
   Key Learning - Ethical cost management is crucial

4. Volkswagen
   Nature of Fraud - Emission data manipulation
   CMA Role - Cost vs compliance trade-off mismanaged
   Key Learning- Ignoring compliance cost leads to larger fraud risks

5. Wirecard
   Nature of Fraud - Fake revenues (~€1.9 billion missing cash)
   CMA Relevance - Transaction & cost flow inconsistencies
   Key Learning - Data analytics (CMA + tech) is key to detection

6. Lehman Brothers
   Nature of Fraud - Use of Repo 105 to hide liabilities
   CMA Role - Misrepresentation of financial position
   Key Learning - CMA's financial structuring insights could detect such window dressing

7. Parmalat
   Nature of Fraud - Fake bank accounts & inflated assets (€14 billion)
   CMA Relevance - Lack of verification of financial & cost data
   Key Learning - Independent cost and fund validation is essential

   Key Takeaways from All Case Studies -
   # Most frauds start as small control failures
   # Lack of cost transparency is a common trigger
   # Early warning signals always exist-but are often ignored
   CMA tools like variance analysis, cost audit and analytics could have prevented or reduced impact.
   "चिन्तनं विनाऽवबोधनम् न सम्भवति"
   (Without analysis, understanding is impossible)

   Final Insight for Professionals
   These cases clearly prove -
   # Fraud is not just an accounting issue-it is a system failure
   # CMA is uniquely positioned to act as a preventive force
   The profession must move from recording costs → questioning costs → protecting value
   "Be the professional who detects the smoke before the fire spreads." !!!

11. Future of Fraud Prevention

The future will see -
AI-driven audits
Real-time fraud detection

Increased regulatory scrutiny
Global compliance standards
#'Integration of finance & technology

Role of CMA in Future -
Becoming Fraud Risk Architects
Leading data-driven governance
Advising boards on risk mitigation
“The future belongs to those who can see risks before they become reality.” !!!

12. Conclusion - A Wake-Up Call

Fraud is not just a financial crime-it is a breach of trust.
A CMA is not merely a cost accountant. He is -
A guardian of efficiency
A watchdog of integrity
A strategic protector of value
“धर्मो रक्षति रक्षितः”
(Those who protect righteousness are themselves protected.)
To every new entrant -
Do not limit yourself to books and exams. # Step into the real battlefield of business ethics and financial integrity.
“Be the professional who not only counts money-but also protects its truth.”!!!

References -

1) Institute of Cost Accountants of India. (Year varies). Cost audit and assurance standards & guidance notes. ICMAI.
2) Association of Certified Fraud Examiners. (2024). Report to the Nations: Global study on occupational fraud and abuse. ACFE.
3) Committee of Sponsoring Organizations of the Treadway Commission. (2013). Internal control-Integrated framework. COSO.
4) Companies Act 2013 India. (2013). Companies Act, 2013. Government of India.
5) Securities and Exchange Board of India. (Year varies). Listing obligations and disclosure requirements (LODR) regulations. SEBI.
6) International Federation of Accountants. (2018). International code of ethics for professional accountants. IFAC.
7) World Bank, & International Monetary Fund. (Year varies). Reports on financial integrity, fraud risk and governance.

Future Role of CMAs in a Risk-Driven World

In today’s evolving business landscape, marked by increased regulatory scrutiny, global compliance standards, and the seamless integration of finance with technology, the role of a CMA is undergoing a significant transformation. No longer limited to traditional accounting functions, CMAs are emerging as fraud risk architects who proactively identify and mitigate risks before they escalate into major issues. They play a key role in leading data-driven governance and advising boards on strategic risk management and compliance frameworks.

Fraud is not merely a financial crime—it is a serious breach of trust that can damage an organization’s reputation and stakeholder confidence. In such an environment, a CMA becomes a guardian of efficiency, a watchdog of integrity, and a strategic protector of value. Their role extends beyond numbers to ensuring ethical practices and transparency in every financial decision.

This is a wake-up call for new entrants. Do not confine yourself to books and exams. Step into the real battlefield of business ethics and financial integrity. As rightly said, “धर्मो रक्षति रक्षितः”—those who protect righteousness are themselves protected. Be the professional who not only counts money but also safeguards its truth.

Written by,

Dr. Dileep Kumar S. D.

Mob -8747831460
Email - dileepsd87@gmail.com

Digital Forensic Auditing: Combating Cyber and Financial Crimes

Abstract:

The convergence of digital technology and financial systems has dramatically expanded the landscape of criminal activity. Digital forensic auditing has emerged as an essential interdisciplinary discipline that bridges conventional auditing with cyber-security and digital evidence analysis to detect, investigate, and prevent both cyber and financial crimes. In this context, the foundational principles of digital forensic auditing, its methodological frameworks, key tools, and practical applications in combating fraud, money laundering, ransomware attacks, and insider threats. It further explores the evidentiary standards that govern digital forensic evidence, regulatory compliance requirements, and the evolving challenges that practitioners face in a cloud-dominated and encryption-heavy environment.

Introduction:

The rapid digitization of economic activity, financial transactions, and organizational communication has created unprecedented opportunities for criminal exploitation. Cybercriminals, fraudulent insiders, and organized financial crime networks increasingly exploit digital vulnerabilities to perpetrate crimes that span national boundaries and jurisdictions.

According to the Association of Certified Fraud Examiners (ACFE), organizations lose an estimated 5% of annual revenues to occupational fraud, and financial crimes enabled by technology have been growing at an accelerated pace (ACFE, 2022). In parallel, the global cost of cybercrime is projected to reach $10.5 trillion annually by 2025 (Morgan, 2020). Against this backdrop, digital forensic auditing has evolved into a critical discipline that integrates the investigative rigor of forensic accounting with the technical precision of digital forensics. Unlike traditional auditing, which primarily assesses financial records for compliance and accuracy, digital forensic auditing seeks to uncover concealed wrongdoing, reconstruct sequences of events from digital artifacts, and produce evidence that is legally admissible in court proceedings. This intersection of accounting, law, and computer science demands both specialized expertise and robust methodological frameworks.

Digital Forensic Auditing – A Conceptual Overview

Digital forensic auditing can be defined as the systematic identification, collection, preservation, examination, analysis, and presentation of digital evidence to support auditing objectives and legal proceedings. It draws upon two parent disciplines: forensic accounting, which applies accounting and investigative skills to legal disputes and fraud investigations, and digital forensics, which involves the scientific recovery and analysis of data from electronic devices (Kranacher & Riley, 2019). The synthesis of these disciplines enables auditors to investigate financial irregularities that manifest in digital form whether in enterprise resource planning systems, email communications, transaction logs, or cloud storage environments.

The primary objectives of digital forensic auditing encompass fraud detection and prevention, regulatory compliance verification, data breach investigation, intellectual property theft analysis, insider threat identification, and litigation support. Its scope extends across sectors including banking, healthcare, government, insurance, and corporate enterprises any domain where digital systems mediate financial flows and sensitive data. A comprehensive forensic audit addresses not only the ‘What’ of an incident but the ‘Whom’, ‘When’, ‘How’, and ‘Why’ providing the narrative depth required for both corrective action and legal prosecution.

Methodological Framework

(1) **Digital Forensic Audit Process:** A structured digital forensic audit follows a multi-phase methodology designed to maintain evidence integrity and analytical rigor . The process typically encompasses six stages such as planning and scoping, evidence identification and collection, preservation, examination and analysis, interpretation, and reporting (Casey, 2011). During the

planning phase, auditors define the objectives of the investigation, identify relevant digital systems and data repositories, and establish the legal authority under which the investigation proceeds. Scoping decisions at this stage significantly influence both the efficiency and completeness of the audit. The evidence collection phase requires meticulous documentation, as any lapse in procedure can compromise the admissibility of findings in subsequent legal proceedings.

(2) **Chain of Custody and Evidence Integrity:** Chain of custody is a foundational principle in digital forensic auditing. It refers to the chronological documentation of evidence handling tracking who accessed the evidence, when, and what actions were taken. This documentation establishes the integrity and authenticity of digital evidence from the moment of collection through its presentation in court. Hash verification using algorithms such as MD5 or SHA-256 is routinely employed to confirm that digital evidence has not been altered at any point in the investigative process (Carrier, 2003). Failure to maintain chain of custody can result in evidence being deemed inadmissible, potentially undermining an entire investigation.

(3) **Live versus Dead Forensics:** Digital forensic methodologies distinguish between live forensics the collection of volatile data from running systems and dead or post-mortem forensics, which involves analysis of powered-down devices. Live forensics is increasingly critical because significant forensic artifacts, including network connections, running processes, and encryption keys in memory, exist only while a system is operational. As encryption becomes ubiquitous, the window for capturing decrypted data in RAM has become a focal point of modern forensic strategy (Ligh et al., 2014).

Digital Forensic Tools and Technologies

The evolution of digital forensic auditing has been substantially driven by advances in forensic software and hardware. Industry-standard platforms such as EnCase, FTK (Forensic Toolkit), Autopsy, and Cellebrite enable examiners to image storage media, recover deleted files, parse file system metadata, and analyze communication artifacts. Specialized tools such as Volatility support memory forensics, while Wireshark facilitates network traffic analysis. In financial crime investigations, tools like IDEA (Interactive Data Extraction and Analysis) and ACL (Audit Command Language) allow auditors to analyze large transaction datasets for anomalous patterns indicative of fraud or money laundering (Ruan, 2013).

Further, Machine learning and artificial intelligence are increasingly being integrated into forensic platforms to automate anomaly detection, classify malware, and accelerate the review of large document sets in litigation contexts. Natural language processing capabilities assist investigators in identifying suspicious communications patterns across email and messaging archives. These technological developments are expanding both the scale and speed at which forensic investigations can be conducted, though they also introduce questions about algorithmic bias and the interpretability of AI-driven findings in legal proceedings.

Applications/Methods in Combating Specific Crimes

(1) **Financial Statement Fraud:** Digital forensic auditing has demonstrated significant effectiveness in uncovering financial statement fraud the deliberate misrepresentation of an organization's financial position for the purpose of deceiving investors, creditors, or regulators. By analyzing digital audit trails within ERP systems, auditors can identify unauthorized journal entries, retroactive modifications to accounting records, and patterns of round-dollar transactions that deviate from Benford's Law a mathematical principle describing the expected distribution of leading digits in naturally occurring datasets (Nigrini, 2012). Forensic analysis of email communications has been instrumental in establishing the intent and coordination of executives engaged in fraudulent financial reporting.

(2) **Cyber-Enabled Financial Crimes:** Cybercrime increasingly intersects with financial crime. Ransomware attacks, for instance, are not merely data security incidents they carry profound financial implications, including extortion payments, operational disruption costs, and regulatory penalties. Digital forensic investigators analyzing ransomware attacks must reconstruct the attack vector, trace crypto-currency payment flows, and assess the extent of data exfiltration (Beebe & Clark, 2005). Business email compromise (BEC) schemes, which have defrauded organizations of billions of dollars, rely on account takeover or email spoofing to redirect financial transfers. Forensic analysis of email metadata, login records, and transaction approvals is central to such investigations.

Money Laundering and Crypto-currency Investigations: The proliferation of crypto-currencies has complicated anti-money laundering (AML) efforts while simultaneously creating new forensic opportunities. Block-chain's public ledger provides a permanent and immutable record of transactions, enabling forensic investigators to trace the movement of illicitly obtained funds across wallets and exchanges. Specialized block-chain analytics platforms such as Chainalysis and Elliptic have become standard tools in financial crime investigations. However, privacy coins and mixing services present significant challenges by obscuring

transaction trails. Forensic auditors working in this domain must collaborate closely with financial intelligence units and regulators to follow the money through multiple layers of obfuscation (Fanusie & Robinson, 2018).

Legal Framework and Regulatory Compliance

Digital forensic auditing operates within a complex web of legal requirements that vary across jurisdictions. Evidence obtained through digital forensic means must satisfy standards of admissibility typically requiring relevance, reliability, and authenticity. In many jurisdictions, these standards are grounded in rules of evidence that were developed for physical evidence and have been adapted, often imperfectly, to digital contexts. The Federal Rules of Evidence in the United States, for example, have been amended to address electronic records, but questions of authentication and hearsay continue to generate litigation (Mason, 2012.

Moreover, regulatory frameworks such as the Sarbanes-Oxley Act (SOX), the General Data Protection Regulation (GDPR), and the Payment Card Industry Data Security Standard (PCI DSS) impose specific requirements on organizations to maintain audit trails, protect data integrity, and respond to data breaches. Digital forensic auditors must navigate these requirements carefully, particularly where privacy laws limit the collection and processing of personal data in the course of an investigation. Cross-border investigations introduce additional complexity, as data sovereignty laws may restrict the transfer of forensic evidence across national boundaries.

Emerging Challenges/Operational Constraints

Despite its considerable capabilities, digital forensic auditing faces a set of persistent and emerging challenges that complicate investigations and constrain the reliability of findings. The exponential growth in data volumes driven by cloud computing, Internet of Things (IoT) devices, and big data analytics means that investigators must contend with datasets of a scale that exceeds traditional forensic processing capacity. Cloud environments, in particular, pose jurisdictional and technical challenges: data may be distributed across multiple physical locations, managed by third-party providers under complex service agreements, and subject to deletion or modification by the provider without the customer's knowledge (Quick & Choo, 2014).

End-to-end encryption, while essential for individual privacy and organizational security, can render communications and stored data inaccessible to forensic investigators without appropriate legal process or cooperation from technology providers. Anti-forensic techniques deliberate efforts by perpetrators to destroy, alter, or conceal digital evidence are becoming increasingly sophisticated, employing steganography, time-stomping, and secure deletion to frustrate investigations. Finally, the global shortage of qualified digital forensic professionals constrains organizational capacity to conduct thorough investigations, particularly among small and medium-sized enterprises.

Recommendations Offered and Future Directions

(1) Organizations seeking to strengthen their forensic audit capabilities should adopt a proactive posture rather than treating forensic investigation as a purely reactive function. This begins with establishing comprehensive digital audit trails across all critical systems, ensuring that logging is enabled, tamper-evident, and retained for periods sufficient to support retrospective investigations. Security information and event management (SIEM) systems should be configured to alert on behavioral anomalies that may indicate insider threats or external intrusions.

(2) Forensic readiness planning the process of ensuring that an organization is prepared to conduct a forensic investigation if required should be embedded within enterprise risk management frameworks. This includes maintaining up-to-date asset inventories, establishing incident response procedures, training personnel in evidence preservation, and retaining relationships with external forensic specialists. Regulatory bodies and professional accounting organizations should continue developing standardized methodologies and certification frameworks to raise the professional competence of forensic auditors globally.

(3) The integration of artificial intelligence in forensic auditing holds considerable promise for automating anomaly detection and accelerating large-scale investigations. However, the deployment of such systems must be accompanied by rigorous validation processes and transparency mechanisms to ensure that AI-generated findings can withstand legal scrutiny. Interdisciplinary collaboration between accountants, lawyers, cyber-security professionals, and data scientists will be essential to meet the evolving challenges posed by sophisticated financial crime in the digital era.

Conclusion:

Digital forensic auditing represents one of the most consequential frontiers in the contemporary struggle against financial and cybercrime. By systematically recovering and analyzing digital evidence, forensic auditors provide organizations, regulators, and law enforcement agencies with the investigative intelligence necessary to identify wrongdoing, recover assets, prosecute offenders, and strengthen preventive controls. As digital systems become ever more central to economic life, the importance of this discipline will only grow. The effectiveness of digital forensic auditing depends upon the continuous development of professional standards, technological capabilities, legal frameworks, and interdisciplinary competencies. Organizations that recognize forensic auditing not merely as a compliance obligation but as a strategic investment in integrity and resilience will be best positioned to navigate the complex threat landscape of the twenty-first century.

References

- Association of Certified Fraud Examiners (ACFE). (2022). Report to the nations: 2022 global study on occupational fraud and abuse. ACFE.
- Beebe, N. L., & Clark, J. G. (2005). A hierarchical, objectives-based framework for the digital investigations process. Digital Investigation, 2(2), 147–167. https://doi.org/10.1016/j.diin.2005.01.002
- Carrier, B. (2003). Defining digital forensic examination and analysis tools using abstraction layers. International Journal of Digital Evidence, 1(4), 1–12.
- Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers, and the internet (3rd ed.). Academic Press.
- Fanusie, Y. J., & Robinson, T. (2018). Bitcoin laundering: An analysis of illicit flows into digital currency services. Center on Sanctions and Illicit Finance. Foundation for Defense of Democracies.
- Kranacher, M.-J., & Riley, R. (2019). Forensic accounting and fraud examination (2nd ed.). Wiley.

Written by,

Shivanjali Suresh Bodke

Mob - 8459625685
Email - shivanjalibodke@gmail.com

Cybersecurity, Forensic Audit, and Digital Vigilance

The rapid digitalization of financial systems has redefined the risk landscape for modern organizations. Traditional control mechanisms alone are no longer sufficient to address emerging cyber threats and complex financial frauds.

Imagine a situation where an organization loses critical financial data overnight or faces a sudden cyberattack that disrupts its operations. Such incidents are no longer rare but have become a growing reality in the digital world. In this environment, Cybersecurity, forensic audit, and digital vigilance are no longer optional safeguards but essential pillars of risk governance.

In the present digital environment, organizations are increasingly exposed to cyber threats, financial frauds and data related risks due to growing dependence on technology.

Let us understand in brief the core of the theme-
Cyber Security: Cyber security focuses on safeguarding systems, networks and financial information from unauthorized access, cyberattacks and data breaches.

Forensic Audit: It involves systematic examination and investigation of financial records and digital evidence to detect fraud and support legal proceedings.

Digital Vigilance: Digital vigilance ensures continuous monitoring and control over digital transactions and activities, thereby enhancing transparency, accountability, and compliance.

Collectively, these elements help organizations strengthen internal controls and ensure sustainable and secure operations.

Risk Governance Frameworks

Risk governance frameworks provide a structured approach to identifying, assessing, and managing risks. In the digital era, organizations must address cyber risks along with financial and operational risks.

An effective framework includes:

- Strong internal controls and policies
- Regular risk assessments
- Compliance with regulatory requirements
- Clear roles and accountability

Such frameworks enable organizations to proactively manage risks and reduce vulnerabilities.

Further, regulatory compliance plays a crucial role in risk governance. Organizations must adhere to data protection laws, cybersecurity standards and financial reporting requirements. A robust governance framework not only minimizes risks but also enhances stakeholder confidence and organizational credibility.

Cyber Resilience Strategies

Cyber resilience focuses on an organization's ability to prevent, respond to, and recover from cyber incidents. It ensures business continuity even in the face of disruptions.

Key strategies include:

- Implementation of advanced cybersecurity systems
- Regular system audits and vulnerability testing
- Employee awareness and training
- Incident response and recovery planning

A resilient organization can quickly recover from cyberattacks and maintain operational stability.

Data Breach Costing and Financial Impact

Data breaches have become a significant concern for organizations, resulting in substantial financial and reputational losses. Understanding the cost implications of data breaches is essential for effective decision making and resource allocation.

The costs associated with data breaches can be broadly categorized into direct and indirect costs. Direct costs include legal penalties, regulatory fines, investigation expenses, and system repair costs. Indirect costs, on the other hand, include loss of customer trust, damage to brand reputation, and business disruption.

From a financial perspective, data breach costing helps organizations evaluate the economic impact of cyber incidents and justify investments in cybersecurity infrastructure. It also assists in budgeting and cost control by identifying areas where preventive measures can reduce potential losses.

Thus, data breach costing is not merely a financial exercise but a strategic tool for enhancing organizational resilience and sustainability.

Digital Forensic Techniques in Fraud Detection

Digital forensic audit is essential for detecting and investigating cyber fraud. It involves collecting and analysing digital evidence to identify irregularities.

Common techniques include:

- Transaction and log analysis
- Email and communication tracking
- Data recovery and examination
- Use of specialized forensic tools

These techniques help organizations trace fraud, identify responsible parties, and support legal proceedings.

Role of CMA in Fraud Prevention and Digital Vigilance

Cost and Management Accountants (CMAs) play a crucial role in strengthening digital vigilance and preventing fraud. Their expertise in financial analysis and control systems adds significant value.

CMAs contribute by:

- Designing effective internal control systems
- Conducting risk assessments
- Monitoring financial transactions
- Evaluating the financial impact of cyber incidents
- Supporting forensic audits

Their role bridges the gap between financial management and cybersecurity. Furthermore, CMAs ensure compliance with regulatory requirements and promote transparency and accountability in organizational operations. Their role as financial strategists makes them integral to the process of fraud prevention and digital vigilance.

Integrated Approach to Risk Management

An effective risk management strategy requires an integrated approach that combines cybersecurity, forensic audit, and digital vigilance. Organizations must align their technological capabilities with financial and governance frameworks to address emerging risks.

Integration ensures that risks are identified and managed holistically rather than in isolation. Such an approach not only enhances operational efficiency but also strengthens organizational resilience and long term sustainability.

Conclusion

In today's digital world, cybersecurity, forensic audit and digital vigilance have become essential for protecting organizations from risks and fraud. With increasing use of technology, businesses must focus on strong control systems and continuous monitoring to ensure safety and transparency.

Cybersecurity helps in preventing attacks, forensic audit supports in detecting and investigating fraud, and digital vigilance ensures regular oversight of activities. Together, they create a strong system for effective risk management.
CMAs play an important role in this process by strengthening internal controls, analysing financial impact and supporting fraud prevention. By adopting these practices, organizations can operate securely and achieve long term stability and growth.

WIRC WELCOMES NEW ASSOCIATE MEMBERS - MARCH 2026

Sl No	M/Ship No	Name	City
1	59447	Anisha Ambalal Awari	Ahmedabad
2	59396	Kuldeepsingh Charansingh Chauhan	Ambarnath
3	59334	Om Naresh Potalwad	Aurangabad
4	59528	Bhakti Ravindra Dandawate	Aurangabad
5	59474	Ritik Singh Ahirwar	Bhopal
6	59471	Om Harshad Pokar	Dombivli
7	59472	Jash Rajesh Chheda	Dombivli
8	59464	Khushboo Kirit Soni	Gandhinagar
9	59393	Yash Jignesh Gor	Goregaon
10	59357	Rimpak Vishwakarma	Indore
11	59527	Prasad Chandrashekhar Wadavane	Kalyan
12	59484	Mangesh Venkatrao Dhepe	Latur
13	59402	Siddhesh Dilip Katkar	Malvan
14	59440	Roshan Govind Kadam	Mumbai
15	59451	Heth Kirti Bhagat	Mumbai
16	59467	Harshad Dinkar Gadhave	Mumbai
17	59445	Harshal Manoj Tank	Mumbai
18	59348	Alvisia Anthony Dsouza	Mumbai
19	59423	Raju Shrinivas Bhandari	Mumbai
20	59457	Uday Rupesh Gupta	Mumbai
21	59479	Manish Mohan Pariyar	Mumbai
22	59412	Vinod Navratmal Bamb	Nagpur
23	59443	Saurabh Vivek Sonatkar	Nagpur
24	59374	Suyog Sudhakar Malpure	Nashik
25	59502	Vidula Vibhav Kamble	Panvel
26	59377	Gourav Kumar Dwivedi	Pune
27	59432	Hanamant Mahadeo Jamadade	Pune
28	59368	Dipak Tanaji Ghadge	Pune
29	59422	Rahul Dattatraya Padalkar	Pune
30	59362	Divya Sabaji Gawde	Pune
31	59349	Pranay Vijay Bhosale	Thane
32	59405	Shilpa Bhalachandra Nayak	Thane
33	59400	Vivek Rajan Gharat	Uran
34	59379	Parth Rajendra Talajia	Vapi
35	59456	Nanji Shamji Baldaniya	Vapi
36	59524	Sagar Voraram Choudhary	Virar

Written by,

CMA Maithili Malpure

Mob - 9421514777

Email - cma.maithilimalpure@gmail.com

Cyber Risk Costing, Digital Forensic Audit and Risk Governance: Expanding the Strategic Role of Cost and Management Accountants

Abstract

Digital transformation has significantly enhanced organisational efficiency while simultaneously expanding exposure to cyber risks with measurable financial consequences. Cyber incidents now create direct cost implications through operational disruption, regulatory penalties, forensic investigation expenses, legal liabilities and reputational erosion.

As organisations increasingly view cybersecurity through a financial risk lens, Cost and Management Accountants (CMAs) are uniquely positioned to contribute through cyber risk costing, digital forensic audit support and governance analytics. Their expertise in cost structures, internal controls and performance measurement enables financial interpretation of cyber incidents, an area often underdeveloped in traditional cybersecurity frameworks.

This article explores the emerging strategic role of CMAs in quantifying cyber risk exposure, strengthening digital control environments and supporting forensic investigations through financial analytics. It further proposes a competency roadmap for CMAs to remain professionally relevant in an increasingly risk-driven and technology-integrated business environment.

The paper argues that the CMA profession is well positioned to evolve from cost efficiency specialists into digital risk finance advisors contributing to enterprise resilience.

Keywords

Cyber Risk Costing, Digital Forensic Audit, Enterprise Risk Management, Fraud Analytics, Digital Governance, Cost Audit, Cyber Resilience, Risk Analytics.

Introduction: Cyber Risk as a Financial Risk Event

Digitalisation has fundamentally altered the risk landscape of modern enterprises. The rapid adoption of ERP platforms, digital payments, cloud infrastructure and AI driven processes has expanded operational capability while introducing new vulnerabilities. Global risk reports increasingly classify cyber incidents among the top business risks rather than purely technological concerns.

The financial implications typically arise through:

Risk Event	Financial Impact
Ransomware attack	Business interruption losses
Data breach	Legal liabilities and penalties
Payment fraud	Direct financial losses
System compromise	Recovery and investigation costs
Reputation damage	Customer attrition cost

This evolution indicates a conceptual shift:
Cyber Risk → Business Risk → Financial Risk
This progression naturally expands the CMA's contribution into financial risk interpretation.

The Concept of Cyber Risk Costing

Cyber risk costing involves identification and measurement of financial exposure arising from cyber threats. A useful analytical structure can be adapted from the Cost of Quality model used in management accounting.

Cyber Risk Cost Architecture

- PREVENTION COSTS (Security investment & training)
- DETECTION COSTS (Monitoring & analytics)
- INTERNAL FAILURE COSTS (System recovery & disruption)
- EXTERNAL FAILURE COSTS (Penalties & reputation loss)

Structured Cyber Cost Classification

Prevention Costs

Proactive investments designed to reduce cyber exposure:

- Security software deployment
- Employee awareness training
- Penetration testing
- Access control design
- Cyber policy development

Detection Costs

Costs incurred in identifying incidents early:

- Continuous monitoring systems
- Internal audit analytics
- SIEM monitoring tools
- Exception reporting systems

Internal Failure Costs

Financial impact before external exposure:

- Data restoration expenses
- Productivity loss
- IT recovery efforts
- Investigation costs

External Failure Costs

Visible financial damage:

- Regulatory penalties
- Litigation costs
- Customer compensation
- Market reputation damage

Strategic Cost Insight for Management

Many organisations treat cybersecurity purely as an IT cost because financial exposure remains unquantified. CMAs can transform decision making by demonstrating:

Preventive Investment is often significantly lower than failure impact.

This allows cybersecurity to be viewed as:

Risk mitigation investment rather than technology expenditure.

Digital Forensic Audit: Expanding the Assurance Role of CMAs

Digital forensic audit integrates financial investigation with digital evidence review. While cybersecurity experts identify technical vulnerabilities, financial professionals quantify consequences. CMAs already possess core forensic competencies including:

- Variance analysis
- Cost behaviour analysis
- Internal control review

- Fraud risk assessment
- Transaction testing

These skills translate naturally into digital forensic environments.

CMA Contribution Areas

Fraud Analytics- CMAs can identify:

- Duplicate payments
- Shell vendors
- Suspicious cost allocations
- Unusual transaction patterns

Digital Transaction Verification - Financial expertise supports:

- Transaction trail validation
- Exception reporting review
- Approval hierarchy testing
- Audit log financial relevance

Financial Damage Assessment - Key contribution areas include:

- Loss estimation
- Insurance claim computation
- Business disruption costing
- Damage modelling

Practitioner Observation -

Technical teams answer: How did the breach occur?
Management asks: What did it cost us?
This financial translation represents a high-value CMA contribution.

Risk Governance: A Strategic Expansion Area

Risk governance ensures organisational risks are systematically identified, evaluated and monitored.
Financial measurement remains central to effective governance.

Governance Contributions of CMAs

CMAs can strengthen risk governance through:

- Risk cost modelling
- Control cost optimisation
- Compliance cost visibility
- Risk KPI design
- Board reporting dashboards

CMA Role Across the Three Lines of Defence

Defence Layer	Responsibility	CMA Contribution
First Line	Operations	Cost discipline
Second Line	Risk	Risk analytics
Third Line	Audit	Forensic assurance

CMAs therefore occupy a natural integration point between finance, risk and governance.

CMA Digital Risk Evolution Framework

Professional Evolution Model

TRADITIONAL CMA:	Cost control & compliance
PERFORMANCE CMA	Profitability & efficiency analytics
RISK CMA	Risk cost analytics
DIGITAL RISK CMA	Cyber costing + forensic analytics + governance

This represents capability expansion rather than role replacement.

Digital Vigilance as a Professional Capability

Digital vigilance refers to proactive monitoring of financial risks arising from digital systems.
Future CMAs may benefit from developing awareness across three domains.

Technology Awareness

- ERP control risks
- Cyber fraud mechanisms
- Data analytics basics
- Information security structure

Analytical Capabilities

- Continuous auditing
- Exception analytics
- Predictive indicators
- Fraud pattern detection

Governance Skills

- Risk reporting structures
- Control documentation
- Compliance monitoring
- Ethics evaluation

The CMA role may gradually evolve toward: **Digital Financial Risk Advisor**

Cyber Risk and Cost Audit: A Future Convergence

While cost audit frameworks do not explicitly include cybersecurity, digital risks affect:
Integrity of cost records

- Internal control reliability
- Operational efficiency
- Compliance systems
- Risk disclosures

Possible future integration areas may include:

- Digital control assessment
- Cyber disruption cost analysis
- Technology risk cost disclosure
- Operational resilience costing

Such developments may emerge as part of professional evolution.

Practice Opportunities for CMAs

Cyber risk is creating new advisory opportunities.

Emerging Service Areas

Advisory

- Cyber risk cost assessments
- Digital control reviews
- Fraud diagnostics
- Risk maturity evaluation

Assurance

- Forensic investigations
- Data analytics assurance
- Compliance review
- Internal control testing

Strategic Advisory

- Cyber insurance evaluation
- Business continuity costing
- Governance reporting
- Risk dashboards

Practice Insight

Traditional services focus on compliance. Cyber advisory focuses on:

- Insight
- Prevention
- Value creation

Competency Roadmap

Competency	Future Skill Need	CMA Contribution
Risk Analytics	Data interpretation	Cost discipline
Technology	ERP knowledge	Risk analytics
Forensics	Fraud analytics	Forensic assurance

Future competitiveness will depend on cross-disciplinary understanding.

Case Illustration

Scenario

A mid-sized manufacturing entity experiences ransomware disruption. CMA Financial Assessment

Cost Element	Amount (₹ Lakhs)
Business downtime	35
Data recovery	12
Investigation	8
Legal costs	10
Customer impact	20

Total Loss: ₹85 Lakhs

Proposed earlier security investment: ₹18 Lakhs

Governance Learning - Cyber incident losses were nearly: Five times prevention cost

This type of financial insight strengthens risk governance decisions.

Global Relevance of Cyber Financial Risk

International studies consistently indicate cyber risk as a leading business concern.

Major trends include:

- Increasing ransomware targeting mid-sized firms
- Rising regulatory penalties for data breaches
- Growth in cyber insurance markets
- Board level focus on cyber governance

These trends reinforce the need for financial interpretation of cyber exposure. This creates opportunity for CMAs globally.

Way Forward for the CMA Profession

Professional evolution may require:

- Cyber risk awareness training
- Data analytics integration
- Forensic skill development
- Risk advisory capability
- Governance participation

Future relevance will depend on the profession's ability to interpret digital risks financially rather than purely recording costs historically.

Conclusion

Cyber risks have become financial realities.

This creates a natural expansion pathway for Cost and Management Accountants into cyber risk costing, digital forensic support and governance analytics. By integrating digital awareness with traditional strengths in cost analysis and controls, CMAs can significantly enhance their strategic contribution. The future CMA may not only answer:

What does it cost to operate?

but increasingly:

What does unmanaged digital risk cost the organisation?

This transition may define the next phase of professional evolution.

References:

- Companies Act 2013
- Information Technology Act 2000
- COSO ERM Framework
- ISO 31000 Risk Management
- ISO 27001 Information Security
- ICMAI Cost Audit Rules
- ACFE Fraud Reports
- World Economic Forum Risk Reports

CMA AI Pravesh

The ICMAI AI Strategy & Capacity Building Board of the Institute of Cost Accountants of India organised "CMA AI Pravesh – Deep-Dive into Artificial Intelligence and Machine Learning for Finance and Cost/Management Accounting" at the WIRC Office from 3rd April to 6th April 2026.

In this four-day training workshop, qualified CMAs working in the domains of cost accounting, management accounting, and finance were introduced to the fundamentals of Artificial Intelligence (AI) and Machine Learning (ML) in simple and easy-to-understand terms. The programme also provided insights into various Generative AI tools and their practical applications, enabling participants to enhance their analytical capabilities and adapt to emerging technological trends in the profession.

CMA Rahul S. Dharne and Ms. Rahee Walambe served as the faculty for the workshop and delivered highly insightful and informative sessions.

Written by,

Prof. Dr P K Rajput

Mob - 9979868862
Email - pkrajputcadilapharma@gmail.com

Cyber security, Forensic Audit and Digital Vigilance: A Strategic Imperative in the Digital Era

In a world driven by data, the true strength of an organisation lies not in how much it owns, but in how securely it protects and governs it."

In today's era, where digital transformation outpaces regulation through a hyper-connected ecosystem, modern organisations are no longer defined merely by their physical assets or financial strength; they are defined by their data ecosystem.

As businesses increasingly rely on data, cloud infrastructure and intelligent systems, the risk landscape has expanded exponentially. Cyber threats, insider fraud, ransom ware attacks and data breaches are not isolated disruptions; they are persistent and evolving challenges.

To navigate this perilous landscape, three critical pillars have emerged as the backbone of modern organisational defence: **Cyber security, Forensic Audit** and **Digital Vigilance.**

These disciplines, when integrated with robust risk governance and resilience frameworks, form the backbone of a defensible and trustworthy enterprise that ensures proactive protection, investigative depth and continuous monitoring.

Together, they enable organisations to not only defend against threats but also detect, respond, and recover with agility and confidence.

Risk Governance: The Strategic Compass

At the heart of any robust cyber security strategy lies risk governance, as it provides a structured approach for identifying, assessing, and mitigating risks while ensuring accountability across all levels of the organisation.

Organisations today establish dedicated leadership roles as Chief Information Security Officers (CISOs) and risk committees to lead this charge. This ensures that cyber security is embedded into boardroom discussions, thus defining clear roles for risk identification, assessment, and mitigation.

Frameworks like the NIST Risk Management Framework (RMF) enable organisations to align cyber security initiatives with business objectives, which promote a culture where risks are continuously monitored, prioritised based on impact and addressed proactively.

Effective governance transforms cyber security from a technical function into a strategic enabler. It ensures that decisions regarding investments, compliance and operations are made with a clear understanding of digital risks.

Cyber Resilience Frameworks: Building Adaptive Strength

While cyber security focuses on protecting systems, Cyber resilience frameworks prepare organisations to withstand, adapt, and recover from attacks. The NIST Cybersecurity Framework (CSF) 2.0 provides a structured path across six core functions: Govern, Identify, Protect, Detect, Respond and Recover.

Leading frameworks such as the NIST Cyber security Framework and ISO/IEC 27001 provide structured approaches to building resilience. These frameworks revolve around five core principles:

- **Identify** risks and critical assets
- **Protect** systems through safeguards and controls
- **Detect** threats using continuous monitoring
- **Respond** effectively to incidents
- **Recover** swiftly to restore operations

Organisations that adopt these frameworks shift their mind set from prevention alone to preparedness and adaptability.

Investments in technologies such as Security Information and Event Management (SIEM) systems, Endpoint Detection and Response (EDR) and advanced threat intelligence enhance their ability to detect anomalies early and minimise damage.

Equally important is regular employee training, incident response simulations and continuous testing to ensure that organisations are not only technologically prepared but also operationally resilient.

Data Breach Costing: Understanding the Financial Impact

One of the most compelling reasons for strengthening cyber security is the **cost of data breaches.** The financial implications of a breach extend far beyond immediate technical recovery.

Global studies indicate that the average cost of a data breach runs into millions of dollars, with certain industries such as healthcare and finance facing even higher impacts due to regulatory penalties and the sensitivity of data.

As of 2024, the global average cost per breach reached **$4.88 million**, with the United States leading at **$9.36 million** per incident. Updated 2025 figures show a global average of **$4.4 million**, escalating to **$10.22 million** in the U.S. due to detection, response, and lost business costs. In the Middle East, incidents cost **$8.75 million**, while European costs vary from **$3.73 million** in France to **$5.9 million** in Benelux.

Organisations that invest in early detection and strong resilience frameworks can significantly reduce these costs. In fact, timely identification and response can lower breach-related expenses by a substantial margin, highlighting the importance of proactive cyber security strategies.

Digital Forensic Techniques: The Investigative Backbone

When incidents occur, the focus shifts from defence to investigation. Digital forensics becomes the cornerstone of investigation and accountability in a legally admissible manner. It involves the systematic collection, preservation, analysis and reporting of digital evidence.

The forensic process typically follows five stages:

1. **Identification** of relevant data sources
2. **Preservation** of evidence to maintain integrity
3. **Extraction** of data without alteration
4. **Analysis** to uncover patterns and anomalies
5. **Reporting** findings in a legally admissible format

Advanced forensic Key techniques include:

- **Disk imaging and Memory Forensics** to create exact replicas of storage devices
- **Timeline Reconstruction and Log analysis** to trace unauthorised access
- **Email forensics** to detect phishing and spoofing
- **Network forensics** to monitor data flow and intrusions
- **Malware analysis** to understand attack behaviour

Innovations such as AI-driven analytics and machine learning have further enhanced forensic capabilities, enabling real-time detection of anomalies and predictive insights.

Digital forensics not only helps in identifying the root cause of incidents but also ensures compliance with regulatory requirements and supports legal proceedings. It transforms reactive investigation into proactive intelligence.

CMA's Role in Fraud Prevention: Bridging Finance and Forensics

While technical teams handle the bits and bytes, financial oversight requires a unique blend of accounting acumen and digital investigative skill. This is where Cost and Management Accountants (CMAs) play a pivotal role in fraud prevention. CMAs integrate forensic audit into risk-based strategies, leveraging digital forensics for continuous auditing.

CMAs contribute to several critical areas:

1. **Risk Assessment and Control Design**
   They design robust internal control systems that minimise fraud risks and enhance transparency.

2. **Data Analytics and Fraud Detection**
   Using advanced analytics, CMAs identify anomalies, detect irregular patterns and flag potential fraud indicators.

3. **Forensic Audit Participation**
   CMAs play a vital role in forensic investigations by analysing financial trails, reconstructing transactions and supporting evidence-based conclusions.

4. **Costing of Cyber Risks**
   They evaluate the financial impact of cyber threats, conduct cost-benefit analyses of security investments and assist in budgeting for risk mitigation.

5. **Governance and Compliance**
   CMAs ensure adherence to regulatory frameworks, ethical standards and corporate governance principles.

6. **Strategic Advisory Role**
   As trusted advisors, they guide leadership in making informed decisions regarding cyber security investments, risk mitigation strategies and long-term sustainability.

   By integrating financial intelligence with digital risk management, CMAs elevate the organisation's ability to prevent fraud and respond effectively to cyber threats.

Digital Vigilance: The Continuous Glue

All these elements unify under the banner of **Digital Vigilance**: the continuous, proactive monitoring of digital assets for anomalous activity. It is a culture, not just a system.
Vigilance shifts organisations from periodic audits to real-time threat detection, monitoring for data leakage, fraudulent transactions, and brand impersonation on the dark web.

Challenges and the Road Ahead

Despite advancements, organisations face several challenges, including skill shortages, rapidly evolving threats and increasing regulatory requirements.
Emerging technologies such as artificial intelligence block chain, and zero-trust architectures are reshaping the cyber security landscape.
The future demands continuous learning, investment in advanced tools and a commitment to ethical governance.
Boards and leadership teams must prioritise cyber security as a strategic investment rather than a cost.

The Way Forward

In the digital age, data is the new currency and trust is the new capital. Cyber security, forensic audit and digital vigilance are not optional; they are fundamental to organisational success and sustainability.
Unifying cyber security, forensic audit, and digital vigilance creates robust protection. Risk governance sets the foundation, cyber resilience frameworks build adaptability, forensic audits provide investigative depth and CMAs bridge financial oversight with technical response.
Key challenges, including skill shortages and rapid threat evolution, are being addressed through CMA-led up-skilling and AI-driven forensics.
As we look toward 2026 and beyond, the message is clear. Organisations must prioritise funding for resilience, adopt zero-trust models and embed ethical leadership into every digital decision.

"Cyber security is not just about defending systems; it is about defending trust, integrity and the future of every digital decision we make."

Written by,

CMA Dr. Vidya Parikh

Mob - +65 9839 5551
Email - vidyaparikh@gmail.com

Digital Vigilance - A Shared Responsibility

Introduction

Digital vigilance is the proactive and mindful exercise of being alert and watchful of the digital world around us including being aware of all the digital exchanges engaged in or any information posted or consumed. This is done with the intention of protecting personal data and guarding ourselves from deceptive content and subterfuge thus providing us with more confidence to navigate the digital space securely (Sustainability Directory, 2024). The dictionary meaning of the term 'vigilance' being 'paying attention to notice possible dangers', clearly suggests, that this involves taking the initiative to actively engage rather than passively waiting for a trigger. It is interesting how in common parlance, the term 'vigilance' is often replaced by the word 'surveillance'. Though both are concerned with warding off the dangers of the digital space, one could see subtle differences. As per Manaher (2023), surveillance involves observing, monitoring, recording, gathering information and analysing patterns to ensure security, while vigilance is more about being alert and attentive to potential threats. Surveillance in the digital context can often involve the use of technology and systems to monitor, control and analyse information while vigilance is more about people and organizations using their knowledge and skills and sense of commitment to stay alert so risks and threats if any, can be responded to in a timely manner. Though surveillance and vigilance go hand in hand in the securing the digital world, this article is going to discuss digital vigilance, why it matters today and how it can best succeed when appreciated as a shared responsibility.

The Landscape of Digital Threats and Why Digital Vigilance Matters

Gone are the times when setting up firewall or installing antivirus software made digital system users feel safe (SinglePointGLobal, 2025). With the proliferation of technology in all aspects of our life, attack vectors have increased giving more opportunities to anti-social elements. Today, cyber security threats are more rampant, conducted in a sophisticated manner, and often involve tapping on human behaviour and human errors to launch attacks. With the stakes being high, response times have drastically reduced and it is only constant vigilance that can anticipate and prevent or at least contain the damage. While automated systems and advanced technologies may be deployed to continuously survey the landscape and lookout for abnormal activity, failed login attempts or anomalies in routine patterns of system behaviour, an inadvertent error or a vulnerability exposed by a user can easily expose an entire network and its data to malicious subjects.

As per Morgan (2025), the Cybercrime magazine, damages inflicted by cybercrime amounted globally to almost $10.5 trillion USD in 2025. With an estimated 7.5 billion users of the internet in 2030, the vulnerability to cybercrime is only set to increase (Morgan, 2025). Today's cybercrime landscape is much more complex and more seriously damaging. It includes crypto-crimes, ransomware, and denial of service and is even moving to AI-enabled cyber-attacks. The spread of misinformation through social media networks, causing chaos, social disturbances and disruptions is another form of cyber-attack. While the intricacy of the attacks and the magnitude of potential losses are huge, the attack vectors are often found to be exploiting human bias and behaviour, making humans the weakest link in the cyber security chain. Phishing, that involves impersonating someone that the user trusts, to get them to reveal passwords, or social engineering, where users are manipulated by luring or scaring them to reveal private and confidential information are common forms of digital crimes that attackers are using to gain access to systems. Visual impostors and deep fake audio and video are also used to distract and beguile users. One wrong move by an unassuming user because of naivety, ignorance, lack of awareness or negligence, can put an individual, organization or even an entire nation at risk. This clearly elicits the need for digital vigilance as a basic requirement of maintaining safe digital spaces and also underscores the fact that digital vigilance is not something to be left to the Information Technology department alone. Digital vigilance needs to be incorporated at individual level, organizational level and even at a community or national level, to be really effective.

Digital Vigilance at the Individual Level

Every individual user of technology needs to see themselves as the first line of defence against an impending cyber-attack. Individuals can demonstrate digital vigilance in many simple ways (Madgula, 2025):

- By maintaining good cyber hygiene practices including the use of strong passwords that are changed at regular intervals.
- Using multi-factor authentication or passkeys
- Decluttering digital space by reducing exposure to unnecessary applications and subscriptions.
- Simply exercising restraint in clicking on links and websites or downloading applications onto devices, and critically analysing such requests before complying is a great form of digital vigilance that every individual can adopt.

Then again, such vigilance is not to be seen as a one-time activity but to be inculcated as an uninterrupted habit in one's digital behaviour. For individuals, being open to continuous learning and developing awareness of the changing digital landscape is key to continuing digital vigilance effectively.

Organizational Responsibility in Vigilance

While individuals can take on the commitment to digital vigilance, it does not absolve the organization of its own responsibilities. Organizational responsibilities can include the following:

- Introducing policies for developing a culture of good cyber security practices.
- Allocating sufficient resources for introducing integrated technologies for robust tech-savvy vigilance and surveillance.
- Ensuring strict compliance to regulatory standards related to data protection and security.
- Arranging for regular and effective trainings for users to raise awareness, and caution them on the emerging risks, is squarely the responsibility of organizational leadership and management.

It is important to remember that none of this can happen without leadership buy-in and stewardship for shared digital vigilance and employee empowerment.

National and Community Responsibilities

The evolving digital ecosystem and the increased connectivity of devices and systems have increased vulnerabilities and raised the risk of more victims falling prey to cybercrime. As we may have seen, the fallouts of such crimes are not restricted to individual losses but can often infiltrate entire networks, even include cross border attacks, causing massive community/national losses. The role of the government at all levels is essential in establishing the right strategic roadmap to digital vigilance.

- Establishment and /or adoption of global standards and regulations such as the NIST (National Institute of Standards and Technology) Cybersecurity Framework and the EU Cybersecurity Act are key measures to support digital vigilance as they provide common pathways and structured controls that diminish risk and increase trust.

- In Singapore, the Monetary Authority of Singapore has established the Shared Responsibility Framework (SRF) where roles, responsibilities and appropriate duties have been designed for consumers, financial institutions, and telecom companies to mitigate phishing and other financial scams and accountability assigned to each party in the event of losses incurred for breached duties.

- Government role in public education and awareness generation cannot be undermined as it goes a long way in building a culture of digital vigilance.

- Leveraging social media platforms and applications by law enforcement organisations to enhance communication and collaboration between authorities and the general public and to encourage community participation in efforts to maintain public safety have fundamentally transformed digital vigilance in societies (Ranaweera, 2024).

- Beneficial partnerships by the government to harness the expertise and resources of academia and the private sector in building secure digital infrastructure capabilities and strengthening digital ecosystems are vital aspects of vigilance (Chinn et al., 2018).

Government leaders need to be conscious of the fact that a big part of a nation's prosperity and national security lies in providing a safe digital environment. This includes prevention of cyber-related crime and protection of critical national infrastructure while also encouraging technological progress and digital advancements (Chinn et al., 2018).

Conclusion

Digital vigilance is no longer optional—it is essential and it is a continuous activity. In this regard, it is also important to view digital vigilance as a shared ethic. In a world where one careless click can create ripples across entire networks, one person's vigilance can also strengthen the whole ecosystem. Thus digital vigilance is not to be seen merely as a compliance requirement, or as a burden but rather as a part of everyone's civic duties and an ethical value for each to build as digital citizens. With digital vigilance, individuals, organizations, communities and nations are not only protecting themselves but the entire digital realm. Safeguarding our digital world is our collective responsibility. When stakeholders engage actively in collaborative efforts, it helps to foster better perception of ethical concerns and the need for safeguarding security and privacy, thereby guaranteeing the growth of a more united, vigilant and resilient society amidst rising digital challenges.

References

Chinn, D., Calam, M., Porter, J. F., & Noble, J. (2018, September 19). Asking the right questions to define Government's role in cybersecurity. McKinsey.com. https://www.mckinsey.com/industries/public-sector/our-insights/asking-the-right-questions-to-define-governments-role-in-cybersecurity

Madgula, M. (2025, December 5). Constant vigilance: Why cyber hygiene and digital self-care are important. Sify. https://www.sify.com/security/constant-vigilance-why-cyber-hygiene-and-digital-self-care-are-important/

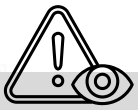
Manaher, S. (2023). Surveillance vs vigilance: How are these words connected?. thecontentauthority.com. https://thecontentauthority.com/blog/surveillance-vs-vigilance

MAS. (2024). Guidelines on Shared Responsibility Framework. MAS.gov.sg. https://www.mas.gov.sg/regulation/guidelines/guidelines-on-shared-responsibility-framework

Morgan, S. (2025, December 11). 2025 Cybersecurity Almanac: 100 facts, figures, predictions and statistics. Cybercrime Magazine. https://cybersecurityventures.com/cybersecurity-almanac-2025/

Ranaweera, N. (2024, November 5). Digital vigilance: Empowering security in the modern world. Faculty of Humanities and Social Sciences. https://fhss.sjp.ac.lk/publication-committee/2024/11/05/digital-vigilance-empowering-security-in-the-modern-world/

SinglePointGLobal. (2025, September 19). Medium. Medium.com. https://medium.com/@cindy_singlepointglobal/following
Sustainability Directory. (2024). Digital Vigilance → area → sustainability. Lifestyle. https://lifestyle.sustainability-directory.com/area/digital-vigilance



Conclusion: Embracing Digital Vigilance

Digital vigilance is no longer optional—it is a continuous and shared responsibility in today's interconnected world. A single careless action can expose entire systems to risk, while one vigilant step can strengthen the security of the whole ecosystem. It should not be viewed merely as a compliance requirement, but as an ethical duty of every digital citizen to protect data, privacy, and trust.

By promoting awareness, collaboration, and responsible digital behavior, individuals, organizations, and communities can build a resilient and secure environment. Active participation from all stakeholders enhances ethical understanding and strengthens safeguards against evolving cyber threats. Ultimately, digital vigilance is a collective commitment that ensures sustainable growth and a safer, more secure digital future for everyone.

As digital transformation continues to accelerate, adopting a proactive approach towards cyber security becomes essential. Continuous learning, regular training, and adapting to emerging threats will empower individuals and organizations to stay ahead of risks. A vigilant mindset not only protects systems but also fosters trust, accountability, and long-term digital sustainability.

WIRC STUDENTS REGIONAL COST CONVENTION 2025

The Students Regional Cost Convention 2026, organised by the Western India Regional Council and hosted by the ICMAI Surat–South Gujarat Chapter, was held on 17th & 18th March 2026 at Platinum Hall, SIECC Auditorium, Surat. The convention proved to be a spectacular and enriching event, bringing together around 800 enthusiastic CMA students from across the Western Region.
This two-day convention offered an excellent blend of knowledge sharing, skill development, and networking opportunities, culminating in its resounding success.

The inauguration ceremony was a momentous occasion, graced by the esteemed presence of distinguished dignitaries, including the Shri Hardik Kothiya, Chairman & Joint Managing Director Rayson Solar Ltd, Chief Guest , Shri Nikhil Madrasi, President, SGCCI, Guest of Honour, CMA TCA Srinivasa Prasad, President ICMAI, CMA Neeraj D Joshi, Vice President - ICMAI, CMA (Dr.) Dhananjay V Joshi, Former President - ICMAI, CMA Mihir N Vyas, Chairman ICMAI-WIRC, CMA Nanty Shah, Vice Chairman - ICMAI WIRC & Convener- SRCC, Chairman Student Coordination Committee, ICMAI-WIRC CMA Chaitanya Laxmanrao Mohrir, Secretary, ICMAI - WIRC, CMA Kishor Vaghela, Chairman - ICMAI Surat South Gujarat Chapter & Co-Convener, SRCC.

The ceremonial lighting of the lamp symbolized the rich Indian tradition of invoking wisdom, positivity, and enlightenment, marking an auspicious beginning to the event.

The first Technical Session, titled “Changing Global Order and Bharat's Role in Multipolarity,” set an insightful tone for the convention. The session was delivered by Dr. Ankit Shah, a distinguished expert in foreign policy and security in the Bharatiya Upmahadweep. The session was highly engaging and thought-provoking, offering students valuable insights into international relations and inspiring them to understand Bharat’s pivotal role in the emerging multipolar world.

Following the Technical Session, a dynamic CMA Skill Sprint Hackathon was organized for the students to provide hands-on learning and practical exposure. The hackathon featured a series of engaging activities, including Excel Setup, MS Excel Competition, Tally Setup, AI Setup, and an AI Competition.

Students actively engaged in these sessions, showcasing their technical proficiency, analytical thinking, and problem-solving abilities. The activities were designed to enhance students’ practical skills in industry-relevant tools such as MS Excel, Tally, and emerging AI technologies. The hackathon created an energetic and competitive environment, encouraging innovation, teamwork, and real-time application of knowledge, making it a highly enriching experience.

This was followed by “CMA Srujan – Talent Competition,” organized for students, wherein participants from across the Western Region showcased their diverse talents through performances such as singing and dancing. The event provided a vibrant platform for students to express their creativity and cultural flair, adding a lively dimension to the convention.

The day concluded with a vibrant cultural evening, bringing together students in a spirit of joy and camaraderie, making it a truly memorable and celebratory experience for all.

The second day commenced with an engaging Mock Parliament, where students deliberated on contemporary and thought-provoking topics such as “Should the Government Regulate Social Media Platforms?” and “Are Women’s Safety Laws Enough in India?”

Participants actively took part in rigorous debates, effectively showcasing their analytical thinking, public speaking skills, and in-depth understanding of the subjects. The session provided a platform for students to express diverse perspectives while fostering awareness on important national issues.

The event was judiciously evaluated by esteemed jury members, CMA (Dr.) Sanjay Bhargave and CMA Amey Tikale, who appreciated the participants for their confidence, clarity of thought, and well-articulated arguments, making the session highly insightful and impactful.

The Mock Parliament was followed by the second Technical Session on “Secrets to a Successful Professional Life,” delivered by CMA Raviraghav Chhavchheria.

In this insightful session, the speaker shared valuable perspectives on building a successful career, emphasizing the importance of continuous learning, discipline, adaptability, and ethical practices. He highlighted key attributes required for professional excellence, such as effective communication, time management, and a proactive mindset.

The session proved to be highly motivating and enriching, offering practical guidance to students aspiring to excel in their professional journey.Bottom of Form

The Valedictory Ceremony marked the formal conclusion of this prestigious convention. The event was graced by esteemed dignitaries including CMA Neeraj D. Joshi, Vice President – ICMAI; CMA (Dr.) Dhananjay Joshi, Past President – ICMAI; CMA (Dr.) Sanjay Bhargave, Mentor – ICMAI-WIRC, CMA Mihir N. Vyas, Chairman – ICMAI-WIRC; CMA Nanty Shah, Vice Chairman – ICMAI-WIRC & Convener – SRCC and CMA Chaitanya Mohrir, Secretary – ICMAI-WIRC.

On this occasion, all the Past Chairmen of the Surat–South Gujarat Chapter were felicitated in recognition of their invaluable contributions and dedicated service towards the growth and development of the profession and the Institute.

The ceremony concluded with a comprehensive summing up of the Convention by CMA Bharat Savani, Former Chairman, ICMAI–Surat South Gujarat Chapter, who reflected on the key highlights and the overall success of the two-day event.

The convention culminated with the Prize Distribution & Felicitation Ceremony, wherein the ICMAI Surat South Gujarat Chapter was honoured for its dedication and meticulous efforts in ensuring the seamless execution of this large-scale event. Prizes were also distributed to the winning students who participated in various competitions, recognizing their outstanding performances and encouraging excellence among participants.

Additionally, the WIRC Staff, ICMAI Surat South Gujarat Chapter Staff, volunteers, supporters, and sponsors were felicitated in recognition of their unwavering support and valuable contributions, which played a pivotal role in making SRCC 2026 a grand success and a truly memorable experience for all participants.

Themes for WIRC Bulletin for the month of May 2026 to October 2026

Month	Theme	Focus Area
May 2026	Cost Audit Excellence: Peer Review and Evolving Standards	Application of Cost Accounting Standards (CAS), practical case studies in peer review, compliance quality, and professional ethics in cost audits.
June 2026	AI, Blockchain & Finance: The Emerging Tech-Accountant	Exploring AI-enabled costing, blockchain transparency, predictive analytics, and automation in management accounting and audits.
July 2026	The Cooperative Economy: Governance, Accountability & Financial Resilience.	Costing in cooperative entities, rural finance reforms, governance challenges, and CMA’s contribution to transparent and efficient cooperative management.
August 2026	Corporate Law and Governance 2026: The New Regulatory Architecture	Independent directors’ roles, SEBI’s related party frameworks, board evaluation, and the evolving compliance ecosystem under the Companies Act
September 2026	Valuation, IBC & Social Audit: The New Dimensions of Governance	Startup valuations, insolvency cost frameworks, social impact audits, and the role of CMAs in ensuring accountability and ethical restructuring.
October 2026	Internal Audit & Risk Management: The Changing DNA of Corporate Control	Strategic risk management, enterprise risk frameworks, internal audit innovations, and CMA’s role in governance and assurance.

CHAPTER NEWS

AHMEDABAD

CMA Practitioner Convention

The CMA Practitioner Convention was organized by the Chapter on February 26, 2026 at Welcome hotel by ITC Hotels, Ahmedabad, as a key inaugural event of the chapter's Diamond Jubilee celebrations (Heerak Mahotsav), commemorating 60 glorious years of excellence and contributions to the CMA profession and India's financial ecosystem.

The convention was inaugurated by CMA Dr. Ghanshyam Trivedi-Director- Xphere Group of Companies, CCM & PD Committee Chairman CMA M K Anand, Past President CCM CMA Ashwin Dalwadi, CCM CMA Chittaranjan Chattopadhyay, CCM Rajendra Bhati, CCM Harshad Deshpande, Chairman of Chapter CMA Mitesh Prajapati, Secretary of Chapter CMA Sunil Tejwani and Chairman of PD Committee of Chapter CMA Uttam Bhandari.

Mr. Devarsh Vakil, Head of prime research at HDFC Securities Ltd talks about smart investment. CA Fenil Shah, RCM, WIRC ICAI speaks about The Next -Gen CMA with AI. He presented “How AI will be helpful” to CMA in their professional work. CMA Rajnedra Bhati was the chairman of the session.

CA Pinal Shah presented on Management Consulting Areas in MSMEs for CMAs. He discussed one case study for better understanding of participation.
CMA J B Mistri presented inventory valuation. CMA Harshad Deshpande was the chairman of the session.

CMA Chittaranjan Chattopadhyay speaks about opportunities for PCMA in banking and insurance sector. CMA Ashish Bhavsar, coordinator of the PD Committee, proposed a vote of thanks.
All the sessions were interactive and very useful to the participant members.

Felicitation Program of Foundation Inter & Final Pass out Students Dec’25 Exam and Yuvotsav

Chapter organized felicitation function at Sardar Patel Smarak, Shahibaug, Ahmedabad for all the students, who have passed Foundation, Intermediate & Final Examination of Dec’25 term. Dr. Neerja A Gupta, Vice Chancellor of Gujarat University was the Chief Guest and CMA Hiranand Savlani, CFO & Executive Director of Astral Ltd was the Guest of Honour in Student’s felicitation program on 27/02/2026. They alongwith Past President CCM CMA Ashwin Dalwadi, CMA Mitesh Prajapati, Chairman,

As a special recognition and honour CMA P D Modh was felicitated by Chief Guest Dr. Neerja A Gupta, Vice Chancellor of Gujarat University for the exemplary role as Oral Coaching Chairman from 1998 to 2020—a remarkable more than two-decade tenure during which he served as a true pillar of strength and his visionary leadership, tireless efforts in guiding countless students, and commitment to quality coaching laid a strong foundation for the Chapter's educational excellence and contributed significantly to its overall growth and reputation.

Thereafter, felicitation of successful students was done by the hand of dignitaries on Dias and committee members, members and faculties.

At the end of the program, CMA Sunil Tejwani, Secretary of Ahmedabad Chapter proposed a vote of thanks. The program concluded with the National Anthem. On completion of the Felicitation function, students of Ahmedabad Chapter showcasing the energy, talent and aspirations performing in Yuvotsav.

Felicitation Program of CMA Achievers, Past Chairpersons and Cultural Evening

Chapter completes 60 years on 28th Feb’2026 and celebrates it as the Diamond Jubilee, the proud and happy reminiscing over 60 glorious years of its existence and growth. To commemorate the long eventful journey of six decades ICMAI Chapter organized a dedicated evening to felicitate the CMAs in recognition of excellence and leadership in profession. Shri Pravin G Mali, Minister of State, Forests and Environment, Climate Change, Transport, Government of Gujarat was the Chief Guest & Mr. Rajendra Patel- Joint Managing Director of Icemake Refrigeration Ltd was the Guest of Honour of the event. Other professional leaders, Corporate

Directors, CFO, Vice Presidents and many more were present during the celebration. The CMA Achievers, all the past chairpersons of Chapter & staff were felicitated by the dignitaries on dais. The Hardil Pandya concert adds value to the proceedings on the program.

CMA Connection Cricket League

CMA Connection Cricket League 2026 for Men and Women tournament organized as a Diamond Jubilee celebration of ICMAI– Ahmedabad Chapter at Clean Bowled Cafe, New Ranip, Ahmedabad on 1st March 2026. The tournament comprises sixteen teams in four groups for men and four teams for women.

The tournament was inaugurated by CMA Mitesh Prajapati – Chairman of Ahmedabad Chapter, CMA Sunil Tejwani - Secretary of Ahmedabad Chapter and Chairman, Sports Committee & CMA Uttam Bhandari. Members and Students participated enthusiastically in this tournament.

Committee Members & Senior Members are present at the concluding event of the tournament. The winning team and the runners-up teams were felicitated by the officials present.

CEP on Importance of financial Literacy, Investment planning, Wealth management for women professionals

On 8th March'2026, on International Women's day, Chapter organized a CEP especially for female CMAs at Chapter premises. CA Vaibhavi Chaniyara & Dr. Bhargavi Khatri were the speakers in the session. CMA Devika Dave, member welcomed the speakers and participant members. She introduced the speakers. CMA Devika Dave and CMA Reena Patadia felicitates the speaker CA Vaibhavi Chaniyara by offering mementos. CMA Devika Dave and CMA Shivangi Shah felicitates the speaker Dr. Bhargavi Khatri by offering mementos. Both the speakers delivered their presentation on the subject. The session was very useful to the participants.

11 Days Advanced Skill Training Program for Final Students of Dec'25 exam term

Chapter organized an 11 days Advanced Skill Training Program for Dec'25 final students from 11th March'2026 to 21st March'2026. In an inaugural session of the Advance Skill Training Program on 11th March'2026, CMA Mitesh Prajapati, Chairman and CMA Sunil Tejwani, Secretary were present. CMA Sunny Patel, Associate Director, Pricewater house coopers Services LLP was the chief guest of the inaugural session. There were many eminent faculties who gave detailed presentation on various topics during the scheduled days, which are useful to the participants in their professional careers.

A valedictory session of the Advanced Skill Training Program was organized on 21st March'2026 at chapter premises. CMA Jalpan Dholakia, General Manager Finance and Chief Cost Officer at Cadila Pharmaceuticals Limited was the Chief Guest of valedictory session.

The participants were felicitated with a "Certificate of Participation" by the dignitaries. CMA Mitesh Prajapati, Chairman proposed vote of thanks.

Webinar on Handling GST Notices- Practical Insights

Chapter organized a CPE Webinar on Handling GST Notices – Practical Insights on 12th March' 2026. CMA Vikas Agrawal was the speaker of the webinar. CMA Ashish Bhavsar-Coordinator, PD Committee introduced and welcomed the speaker as well as participants. The Speaker CMA Vikas Agarwal delivered the presentation in a simple manner, which was very useful to the members. A large number of members participated in the webinar. The session was interactive and informative to the members.

Valedictory Session of CAT Batch (Course No.388-11-2025)

Chapter has organized the Valedictory session of CAT Batch (Course No.388-11-2025) on 13th March' 2026. CMA Mitesh Prajapati, Chairman brief on scope of the CAT course also welcomed the participants during his welcome speech. All the participants were present in the session. The participants were felicitated by participation certificate. CMA Mitesh Prajapati, Chairman proposed vote of thanks.

Participation in Students Regional Cost Convention (SRCC) at Surat

A Large number of students from Chapter participated in Students Regional Cost Convention at Surat on 17th & 18th March'2026 alongwith CMA Mitesh Prajapati, Chairman of Chapter and CMA Ashish Bhavsar, Member. The theme of the convention was Empowered CMAs for Empowered India.

Webinar on Cost Audit – Pharmaceutical Industries

Chapter organized a CPE Webinar on Cost Audit – Pharmaceutical industries on 20th March'2026. CMA Sukrut Mehta was the speaker of the webinar. CMA Mitesh Prajapati, Chairman of Chapter welcomed the speaker as well as participants. CMA Jainil Patadia, member, introduced the speaker. The Speaker CMA Sukrut Mehta delivered the presentation in a simple manner, which was very useful to the members. A large number of members participated in the webinar. The session was interactive and informative to the members. Vote of thanks was proposed by CMA Ashish Bhavsar, Coordinator-PD committee.

CEP on Mind Management

Chapter organized a CPE on Mind Management on 21st March'2026 at Chapter premises. CMA P D Modh was the speaker of the session. CMA Mitesh Prajapati, Chairman of Chapter welcomed the speaker and participants. CMA Yash Jodhani introduced the speaker and CMA Amit Raval felicitated the speaker by offering Memento. The Speaker CMA P D Modh delivered the presentation in a simple manner, which was very useful to the members. A large number of members participated in the session. The session was interactive and informative to the members. CMA Mitesh Prajapati, Chairman proposed vote of thanks.

BARODA

CMA Premier League 2026 – A Grand Success

The 9th season of the CMA Premier League (CMA PL-IX) was successfully organized on 28th February and 1st March 2026 at Aryan Cricket Academy. Six teams participated in the tournament under the theme "A Season like Never Before." After thrilling matches, Dabbang Diwanji emerged as Champions. The league fostered unity, sportsmanship, and camaraderie within the CMA fraternity, blending professional networking with spirited competition.

Webinar on "Strategic Decisions: From Numbers to Value Creation".

Chapter successfully organized an online CPE Programme on "Strategic Decisions: From Numbers to Value Creation" on 6th March 2026. The session was delivered by CA Gaurav Sharma, who shared valuable insights on aligning financial data with strategic decision-making for enhanced value creation. The webinar witnessed an encouraging participation of 113 members, reflecting the keen interest of professionals in strengthening their strategic and analytical capabilities. The session was highly informative and well-received, contributing effectively to the professional development of the participants.

Empowering Voices: Baroda Chapter Celebrates International Women's Day

Chapter hosted a vibrant and inspiring "Women's Day Celebration" on March 7, 2026, at Vanijya Bhavan. The physical event brought together a powerful community of professionals and aspiring accountants. The atmosphere was electric as 8 female members and over 200 enthusiastic female students gathered to honor the achievements of women in the profession. The event featured insightful sessions led by distinguished speakers who shared their expertise and personal journeys:

CMA Amruta Vyas – Chairperson of the Baroda Chapter, who inspired all attendees with her motivating words and leadership. CMA Kiran Mishra provided valuable perspectives on professional excellence. CMA Bhavani Ghattamaneni engaged the audience with her deep industry knowledge. CMA Susheela Maheshwari added to the prestige of the panel, inspiring the next generation of cost accountants.

Convocation for Dec-25 Examination

The Convocation Ceremony held on March 7, 2026, was a proud moment for the ICMAI Baroda Chapter, highlighting the exceptional academic performance of our students from the December 2025 exam term.

The event recognized the pivotal role Cost and Management Accountants (CMAs) play in boosting organizational profitability and efficiency across the manufacturing and service sectors. Chapter celebrated the remarkable achievements of our students: 61 students of Final, 186 students of Intermediate, 265 Students of Foundation felicitated on the occasion.

Among the many success stories in Final Course Mr. Murtuzaali Nayabali Samlayawala secured the top spot for the Baroda Chapter, In Intermediate Course: Jainam Shah achieved Rank 1 locally and earned a prestigious All India Rank 8 with 611 marks and in Foundation Course: Mr. Arman Sanjay Kumar Rana led the foundation batch with a score of 318/400.

These students exemplify the expertise and dedication required of future Cost and Management Accountants to drive business success and organizational efficiency.

Webinar on "S Electric Vehicles - Emerging Business and Financing Models"

On March 9, 2026, the Chapter hosted a specialized online CPE session to explore the future of transportation. The webinar, titled "Electric Vehicles - Emerging Business and Financing Models," attracted a group of 91 members eager to navigate the shifting landscape of climate finance and e-mobility.

The session featured two prominent experts who provided a deep dive into the sector's financial and operational complexities:
Arun Krishnan: Serving as the Program Director for Climate Finance at WRI India, he brought extensive expertise in structuring sustainable financial frameworks.
Sharvari Patki: As the Program Head for Electric Mobility at WRI India, she contributed specialized knowledge on the technical and strategic growth of the electric vehicle industry.

Conducted in collaboration with WRI India and CoEZET IIT Madras, the two-and-a-half-hour program offered members valuable insights into new business models.

Online CPE session titled "Year End Consideration - IDT"

On March 12, 2026, the Chapter hosted an insightful online CPE session titled "Year End Consideration - IDT". The event saw an enthusiastic turnout with 99 members in attendance.

The session was led by two seasoned professionals who shared their deep expertise in the field of indirect taxation. CMA Krunal Solank & CA Basavaraj M were the speakers. The webinar concluded successfully, providing members with practical strategies for handling complex year-end compliance and regulatory challenges.

Online CPE session titled "Merger & Acquisition-Indirect Tax"

On a quiet Monday afternoon in Vadodara, the digital landscape hummed with activity as the Chapter hosted an insightful session on the complexities of modern finance.

On March 16, 2026, a group of 113 members logged in from across the region to delve into the intricate world of "Merger & Acquisition-Indirect Tax". The online forum served as a vital space for professional growth, offering participants 2 CPE Hours for their dedication to staying ahead of industry shifts. CA Jenil Jain was the speaker.

CMA Students Regional Cost Convention (SRCC) 2026

The CMA Students Regional Cost Convention (SRCC) 2026 was more than just a gathering; it was a transformative "movement" toward building an empowered India. Under the theme "Saksham," which represents capability with purpose, 73 dedicated students gathered at the Surat International Exhibition Convention Centre (SIECC) on March 17th and 18th, 2026. Hosted by the ICMAI Surat South Gujarat Chapter, the convention served as a launchpad for these 73 future CMAs to lead tomorrow's India with integrity and vision.

Grand launch of Netram and VISWAS 2.0 (Cluster 4)

The morning of March 21, 2026, carried a sense of transformation for the people of Vadodara. Under the bright, clear sky at the Navlakhi Ground, a massive gathering of students and community members watched as the city took a giant leap into the future. The invitation was for the grand launch of Netram and VISWAS 2.0 (Cluster 4), a sophisticated technological upgrade aimed at keeping Vadodara and Surat safe. This wasn't just a routine ceremony; it represented a massive investment of over ₹172 crore by the Gujarat State Police Housing Corporation and another ₹335 crore for 44 distinct development projects across the district. The Chief Guest, Shri Harsh Sanghavi, the Honorable Deputy Chief Minister of Gujarat, took the stage. He was joined by a long list of dignitaries, including Dr. Manishaben Vakil (Minister of State), Shri Balkrishna Khanderao Shukla (Chief Whip, Gujarat Legislative Assembly), Shri Narasimha Komar, IPS (Police Commissioner), Shri Anil Dhameliya, IAS (Collector of Vadodara. The presence of so many leaders emphasized that this was a milestone for the region's infrastructure and public safety. Among the crowd, the students were the most inspired. For them, the launch of VISWAS 2.0 wasn't just about cameras and software; it was a promise of a smarter, more secure environment to live and study in. As the dignitaries performed the foundation stone-laying ceremony (Khatmuhurat), the cheers from the crowd echoed the shared hope of a progressing Gujarat.

KALYAN AMBERNATH

Ten Days Industry Oriented Training

Chapter organized 10 days Industry Oriented Training commencing on 22nd February 2026 to 4th March 2026 for final students appearing June 2026 examination .CMA Gopichand B. Shamnani, Secretary of chapter welcomed faculty and students and explained how students will be benefited by updated knowledge shared by faculties during 10 days of training.

Eminent and experienced faculties of colleges and professionals were invited to deliver lectures on topics like Working Capital Management, A.I. in Finance Accounting & Auditing , Financially story telling for Future CMA , Cost Records & Cost Audit , Group Communication Skills & Importance Of Team In Working Environment, Receivable Management, Professional Skills For Corporate Success, Introduction to Foreign Exchange and Input Tax Credit under G.S.T. Programme was co-ordinated by Mr. Raju P.C Executive Secretary and Mr. Ravi Rohra Office Assistant.

Prize Distribution Function & Celebration of International Women's Day

On Sunday 8th March 2026 Chapter organized Prize Distribution Function for the Foundation Students passed in December 2025 examination at of Smt. C.H.M. College of Arts, Science & Commerce,

CMA Gopal U. Keswani Chairman of Chapter welcomed the Guests Dr Reshmi Gurnani , Dr. Kajal Bhojwani, Dr. Bhavna Binwani the students and parents. Function started with National Anthem

CMA Gopichand B. Shamnani informed that Dec 2025 exams are declared and 348 students passed CMA Foundation, 256 Students passed CMA Inter and 74 Students passed CMA Final.

Prizes were distributed at the hands of dignitaries.

On the occasion International Women's Day was also celebrated by honouring faculty members with mementos. Meeting ended with vote of Thanks

Joint One Day International Conference with Bharat College

Bharat College of Arts and Commerce, Badlapur, in association with the Institute of Cost Accountants of India (ICMAI) - Kalyan-Ambarnath Chapter successfully organized an International Conference in the Hybrid mode on the theme “Innovation for Sustainable Development – A Multidisciplinary Approach.” On Saturday 21st February, 2026.

CMA Dr. Gopichand Shamnani, Secretary justified his role by welcoming all the national and international guests of the conference.

Keynote Speaker Prof. Iniodu George, University of Cross River State, Calabar, Nigeria honored the conference by sharing his ideas about how innovative practices can be adopted throughout the globe ensuring sustainability. It was an enlightening session with various innovative strategies that can be adopted at individual and social level.

Technical Sessions were chaired by eminent faculties Overall, there were more than 100 registered participants and shortlisted 36 presentations in 4 different sessions due to less time availability.

The valedictory session was graced by eminent dignitaries including CMA Dr. Kulvinder Kaur, CA Rashmi Gurnani, and Dr. Anil Singh, whose presence added prestige and significance to the occasion.

Overall, the International Conference proved to be a significant academic event, reinforcing the institution’s commitment to research excellence and sustainable progress.

PIMPRI CHINCHWAD

International Women’s Day Program on 9.3.2026

On March 9, 2026, Chapter hosted an International Women’s Day celebration at CMA Bhawan.

CMA Rupali Kothavale. Secretary, The ICMAI – Pimpri Chinchwad Chapter welcomed and felicitated guest CMA Dr. Divya Lakhani, HOD - MBA, Sadhu Vaswani Institute of Management Studies for Girls, Pune by offering shawl, Shri phal and memento and CMA Foundation student Ms. Anchal introduced the guest. CMA Balkrishna Hajare, Chairman, The ICMAI – Pimpri Chinchwad Chapter was present during the event.

The event brought together CMA members, professionals, and students to celebrate and appreciate the achievements of women in the field. The program included inspiring talks by accomplished women professionals, engaging panel discussions, and networking sessions that gave everyone a chance to connect and share ideas.

There were also some wonderful performances, games and a special recognition of outstanding women from the community. Overall, the event created a positive and encouraging atmosphere, highlighting the importance of inclusivity, support, and empowerment for everyone.

CultFest 2K26- Students' Felicitation Event

On March 13, 2026 Chapter organized the Students Felicitation Function and Cultural Activities Program (CultFest- 2K26). During the event, anchoring was carried out seamlessly, and all dignitaries on the dais were warmly welcomed, including Chief Guest Shri Mandar Ashok Kelkar, Additional Commissioner, State Tax (SGST), Yerwada, Pune, CMA Neeraj D Joshi, Vice-President, The ICMAI, CMA Mihir Vyas, Chairman, WIRC, The ICMAI, CMA Mahendra Bhombe, Member of WIRC, The ICMAI, CMA Mohandas Nair, Business Controller, Atlas Copco India (Private) Limited, Pune, CMA Ajay Kumar, CFO, Minda Corporation Limited, CMA Dinesh Sahane, Deputy General Manager, Sabros Limited, CMA Sachin Asole, Finance Director, GKN Sinter Metal Private Limited and members of the managing committee Chairman CMA Balkrishna Hajare, Vice-Chairman, CMA Kunal Wakte, Treasurer CMA Guruprasad Kulkarni and P D Committee Chairman CMA Sagar Malpure, CMA Ajit Shinde & CMA R B Laddha.

CMA Mahendra Bhombe highlighted the growing importance of cost accountants in strategic decision-making, emphasizing innovation, problem-solving, and continuous professional development.

CMA Harshad Deshpande delivered an encouraging speech to the students during the felicitation programme. He praised their commitment to the CMA journey and acknowledged the dedication required to reach such milestones. He urged students to apply their knowledge with confidence in real-world scenarios.

CMA Mihir Vyas the students to uphold ethical practices, apply their knowledge confidently, and develop leadership and communication skills essential for professional success. His words inspired the students to aim high and uphold the values of the profession.

CMA Mohandas Nair delivered an inspiring speech to the students during the felicitation function. He further focused on the importance of studying Cost and Management Accounting and highlighted the wide range of opportunities available in the corporate sector.

CMA Dinesh Sahane, in his inspiring speech, beautifully reflected on his journey toward achieving the prestigious CMA qualification. CMA Sachin Asole in his speech highlighted the vital role played by cost accountants in upholding financial prudence and strengthening governance across both public and private sectors. CMA Ajaykumar reflected on the remarkable growth of the Pimpri-Chinchwad Chapter and expressed his joy in witnessing the success of the students.

Vice-President CMA Neeraj Joshi shared valuable practical insights, stressing discipline, analytical thinking, and the importance of staying aligned with evolving industry requirements. Sharing perspectives from his rich industry experience, he highlighted how CMAs are vital to organizational decision-making and strategic growth.

Chief Guest Shri Mandar Ashok Kelkar delivered a thought-provoking address, emphasizing integrity, continuous learning, and the vital role of cost accountants in strengthening financial governance and contributing to the nation's development.

All the speakers collectively appreciated the students' hard work and achievements, inspiring them to strive for excellence and contribute meaningfully to the profession and society.

The students of the Chapter celebrated the cultural program with immense joy, leaving a lasting impression on everyone.

Webinar on 'From Legacy Laws to a Unified Code: Major Provisions of The Securities Markets Code, 2025'
On March 28, 2026, Chapter organized a CEP Webinar on "From Legacy Laws to a Unified Code: Major Provisions of The Securities Markets Code, 2025." through online mode.

CMA Balkrishna Hajare, Chairman of the Chapter welcomed all the audience and speaker CMA CA CS Pankaj Kapoor, Assistant professor SVKM'S NMIMS Chandigarh. CMA Sagar Malpure, P D Committee Chairman, of the Chapter introduced the speaker.

The webinar was expertly conducted by CMA Mr. Kapoor, provided in-depth insights into the key provisions of The Securities Markets Code, 2025, and shared practical perspectives on its anticipated impact on the industry. His detailed analysis and interactive presentation style enriched the session, enabling participants to gain a thorough understanding of the unified code and its implications for professionals and organizations in the securities sector.

The event successfully fostered a deeper understanding of the evolving legal landscape and equipped professionals with actionable insights to navigate the changes effectively.

PUNE

Women's Day on 7th March 2026.
Chapter organized the Women's Day Celebration' at CMA Bhawan, Karve Nagar on 7th March 2026. The theme of the program was "GIVE & GAIN."

Our Chief Guest Dr. Nivedita Ekbote Corporator, Pune Municipal Corporation & Principal, Modern College, and Guest of Honour CMA Suparna Govande Senior Banker with extensive experience in Corporate Credit Management.

On this occasion Chapter for the very first time organised a Neuro Yoga Orientation session by Dr. Sarita Zalkikar, Homeopathic Consultant, Yoga Teacher & Yoga Therapist, and Mrs Janhavi Prabhudesai, Neuro Yoga Teacher & Fitness Expert. Also arranged a free Health Check-up Camp in association with Apollo Hospitals for all Members and Family.

The program commenced with the ceremonial lighting of the lamp by esteemed guests Special Invitee CMA Dhananjay Joshi, Advisors ICMAI, Pune Chapter, CMA Chaitanya Mohrir, Secretary WIRC, ICMAI, CMA Meena Vaidya, CMA Dr Sanjay Bhargave Advisors ICMAI of the Chapter. CMA Shrikant Ippalpalli, Chairman, CMA Rahul Chincholkar Vice Chairman, CMA Himanshu Dave, Secretary ICMAI CMA Tanuja Mantrawadi, Treasure ICMAI,Pune Chapter CMA Anuja Dabhade Managing Committee Members of ICMAI Pune Chapter were present for the programme.

CMA Abhay Deodhar, CMA Sujata Budhkar, CMA Anuradha Dhavalikar and many other female Cost Accountants along with students & members graced the occasion with their presence.

The Women's Day celebration concluded with a cake-cutting ceremony. All the participants thoroughly enjoyed the occasion and the delicious meal. CMA Tanuja Mantrawadi Treasure of ICMAI Pune Chapter and CMA Anuja Dabhade, Managing Committee Members of ICMAI Pune Chapter, took the initiative for the Women's Day Celebration.

Valedictory Session of CAT Course
Chapter conducted the second CAT Course batch (Part I & II) for retiring/retired Armed Forces personnel under DGR from November 2025 to March 2026 at CMA Bhawan, Pune. The Valedictory Session was held on 13th March 2026, CMA Shrikant Ippalpalli, Chairman of the Chapter felicitated Chief Guest LT.GEN.S S Hasabnis PVSM VSM ADC (Retd). CMA Himanshu Dave, Secretary, of the Chapter welcomed the Chief Guest, students. Program started with the lighting of lamp and the Institute's Anthem. Participants were awarded course completion certificates and commended the Pune Chapter for its excellent faculty support, food, and facilities.

Webinar on "Year End Activities in Income Tax and Book Closure"
Chapter successfully organized a webinar on the topic "Year End Activities in Income Tax and Book Closure" on 17th March 2026 via Google Meet.

The session was graced by CMA Amit Shahane as the keynote speaker. His presentation was insightful, the webinar received an overwhelming response from members.

CMA Rahul Chincholkar, Vice-Chairman of the Chapter, warmly welcomed the speaker and attendees, setting a positive tone for the session. The event concluded with a formal also Vote of Thanks delivered by CMA Rahul Chincholkar, Vice Chairman of the ICMAI Pune Chapter, who appreciated the speaker's valuable insights and thanked the participants for their active engagement.
The session proved to be highly informative and was well-received by all attendees.
10 Days Training for Final (IOTP)

Chapter started 10 Days Industry Oriented Training Program (IOTP) for Final students from 28th February 2026 for the Session No.06 (January to June 2026) for Oral & Postal students at CMA Bhawan, Karvenagar.

CMA Himanshu Dave & CMA Amit Shahane were speakers for the inaugural lecture of the program.
Sandeep Joshi, Chapter welcomed the speakers and students for the training. CMA Himanshu Dave, Secretary of the Chapter also guide the participants.

Advance Skill Training Program for Newly Qualified CMA's
Chapter organized the Advance Skill Training Program (ASTP) for newly qualified CMAs of December 2026 from 20th March 2026 to 30th March 2026 at CMA Bhawan, Pune Chapter premises.

A total of 104 students registered for the training, out of which 101 students attended regularly. The chapter conducted more than 29 sessions on various topics, which proved very useful for the newly qualified CMAs. The faculties included practicing Cost Accountants and professionals holding senior positions in industry, who shared their rich experience and knowledge with the participants.

The lectures were lucid, informative, and fruitful, providing practical insights especially helpful for facing campus interviews. The Chapter Managing Committee worked diligently to ensure the success of the program.

On 30th March 2026, the valedictory session was organized. CMA Himanshu Dave Secretary of the Chapter hosting a Program. CMA Pravin Gavali, Divgi Torqtransfer Systems Ltd, a listed tier 1 automotive company Finance Controller, graced the occasion as the Chief Guest. CMA Amit Apte – Former President, ICMAI, graced the occasion as the Guest of honour. CMA (Dr.) D. V. Joshi – Former President, ICMAI, congratulated all the newly qualified CMAs and shared his thoughts on the journey of learning and earning through this course highlighted the significance of pursuing a CMA career, emphasizing the wide range of opportunities it offers in the corporate sector, self-practice, and various other diverse fields.

CMA Shrikant Ippalpalli, Chairman of the Chapter, welcomed the participants and felicitated the Chief Guest. In his address, he reviewed the 12 days of topics and the practical knowledge shared by the faculties. CMA Rahul Chincholkar, Vice chairman - ICMAI Pune Chapter congratulated Newly Qualified CMAs and also expressed his views about topics covered.

CMA Amit Apte, congratulated the newly qualified CMAs and welcomed them to the profession. He shared valuable tips on successfully facing interviews and encouraged them to become members of the Institute.

During the session, the newly qualified CMAs were felicitated with mementos and participation certificates. Some participants expressed their views on the sessions, faculties, topics, food, and overall arrangements, and extended their gratitude to the Managing Committee and Office Staff members

CPE on 'Emerging Professional Opportunities in Sustainability for CMAs'
Chapter jointly with Sustainability Standards Board - ICMAI, successfully organized a Continuing Professional Education (CPE) on 'Emerging Professional Opportunities in Sustainability for CMAs' on 21st March 2026 at CMA Bhawan, Karvenagar.

CMA Himanshu Dave, Secretary of the Chapter, welcomed all participants and introduced the speakers. CMA Tanuja Mantravadi, Treasure of the chapter felicitated the speakers CMA A. Sekar and CMA Anuradha Dhavalikar,

The programme concluded with a Vote of Thanks delivered by CMA Rahul Chincholkar, Vice-Chairman of the Chapter.

CMA Sunil Tejwani, Chief Guest CMA Dr. Ghanshyam Trivedi, CMA Ashwin Dalwadi, Past President & CCM-ICMAI, CMA M K Anand, CCM-ICMAI, CMA Mitesh Prajapati , CMA Uttam Bhandari during CMA Practitioner Convention organised by ICMAI Ahmedabad Chapter on 26th February 2026.

View of Participants during Valedictory Session of CAT Batch held at ICMAI Ahmedabad Chapter on 13th March 2026.

CMA Amruta Vyas – Chairperson of the Baroda Chapter alongwith Successful Students of December 2025 examination during Felicitation programme organised by ICMAI Baroda Chapter on 7th March 2026.

CMA Amruta Vyas – Chairperson of the Baroda Chapter felicitating Winning team of CMA Premier League 2026 organised by Baroda Chapter on 1st March 2026.

Chief Guest Shri Mandar Ashok Kelkar, Additional Commissioner, State Tax (SGST), Yerwada, Pune, lighting the lamp during Students Felicitation Function and Cultural Activities Program (CultFest- 2K26) organised by Pimpri Chinchwad Chapter on 13th March 2026.

Pimpri Chinchwad Chapter celebrated International Women's Day on 9th March 2026.

CMA Amit Apte, Past President, ICMAI & CMA Dr. D. V. Joshi – Past President, ICMAI lighting the lamp during the valedictory session of ASTP held at Pune Chapter

Pune Chapter celebrated International Women's Day on 7th March 2026.

RNI No. 22703/72 Posted at Mumbai Patrika Channel on 10th of every month.
Date of Publication is on 10th of every month. Postal Regn. No. MCS/089/2024-26

WESTERN INDIA REGIONAL COUNCIL

is pleased to announce

3RD REGIONAL TAX CONCLAVE 2026

मंथन

Theme:

Strengthening Economic Growth through Tax reforms and Compliances

Date:
26th April 2026, Sunday

Venue:
MP Hall Bhilai Niwas, Civic center Bhilai

HOSTED BY: ICMAI – BHILAI CHAPTER
CMA BHAWAN, CIVIC CENTRE, BHILAI, CHATTISGARH - 490 006

Non Residential Delegate Fees:

Delegate Categories	Participation Fees
Self-Sponsored Members	700/-
Corporate Delegates	1000/-
Students	400/-

Payment Details

For Cheque or DD	Details of NEFT Payment
The Cheque/DD should be in the favour of **"The Institute of Cost Accountants of India- WIRC".**	Bank of Baroda. Horniman Circle, Mumbai SB Account No: 27940100022156. IFSC Code: BARB0PBBMUM (Fifth Character is ZERO) MICR Code: 400012111. PAN: AAATT9744L GSTIN No. : 27AAATT9744L1ZS

For Registration please contact

Western India Regional Council of ICMAI	ICMAI – Bhilai Chapter
Rohit Chambers, 4th Floor, Janmabhoomi Marg, Fort, Mumbai 400 001. Maharashtra. India. Mob: 9819187416 / 9076020355 Email: wirc.admin@icmai.in	CMA Bhawan, Civic Centre, Bhilai , Chattisgarh, 490 006 Phone: 0788-2222767/ 2898343 Email: bhilai@icmai.in

To,

If undelivered please return to:
THE INSTITUTE OF COST ACCOUNTANTS OF INDIA
WESTERN INDIA REGIONAL COUNCIL,
Rohit Chambers, Janmabhoomi Marg, Fort,
Mumbai 400 001

Printed & Published by Mihir Narayanbhai Vyas on behalf of the Western India Regional Council of the Institute of Cost Accountants of India, Printed at Surekha Press, Gala No. A-20, First Floor, Shalimar Industrial Estate, Matunga Labour Camp, Opp. Tata Power Co., Andhra Valley Road, Matunga, Mumbai 400 019. Published at Western India Regional Council of the Institute of Cost Accountants of India, Office No. 32, Rohit Chambers, 4th Floor, Janmabhoomi Marg, Fort, Dist-Mumbai, Pin Code-400 001, Maharashtra. Tel.: 9372045191, 8828061444, 9372036890 E-mail: wirc.admin@icmai.in Website:www.icmai-wirc.in. Editor:Mihir Narayanbhai Vyas