INSTITUTE OF CHARTERED ACCOUNTANTS OF INDIA | DxFS 2026

Digital Personal Data Protection

Application & Implementation

‘India Joining the Global Data Protection League’

KBS Manian | Group CRO | Apollo Hospitals

Privacy Principles · Global Landscape · DPDP Journey · DPDP vs Global · Takeaways

01 Universal Privacy Principles

THE 7 UNIVERSAL PRIVACY PRINCIPLES — Common to Every Jurisdiction

Lawfulness | **Purpose Limitation** | **Data Minimisation** | **Accuracy**

Storage Limitation | **Security** | **Accountability**

1 Lawful, Fair & Transparent

Processing only with valid consent or for legitimate uses notified in the Act.

2 Purpose Limitation

Use the data only for the specific purpose for which it was collected.

3 Data Minimisation

Collect only what is necessary for the stated purpose — no 'just in case' data.

4 Accuracy

Keep data accurate, complete and up to date; correct on request.

5 Storage Limitation

Retain only as long as necessary for the purpose; erase thereafter.

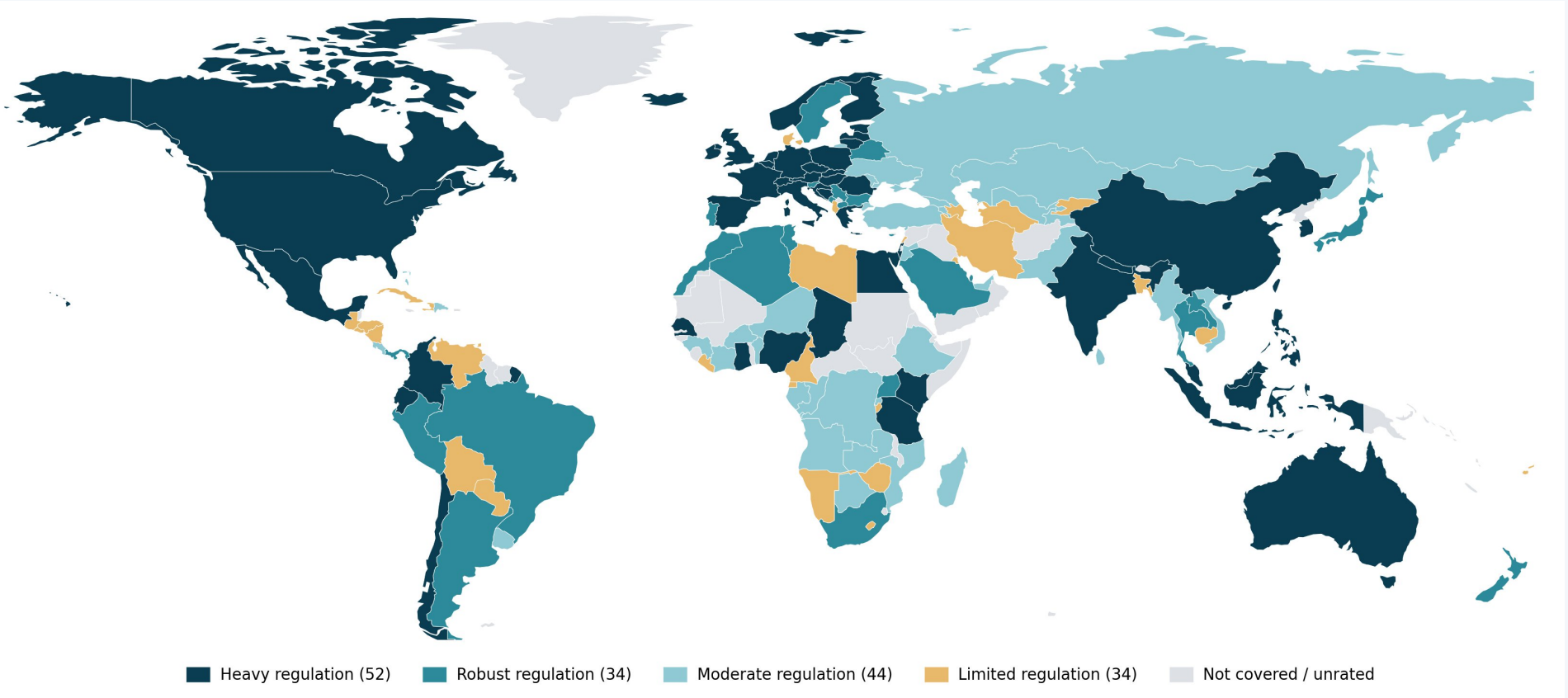
6 Security & Accountability

Implement reasonable safeguards; be answerable for compliance and breaches.

Key Audit Insights

- ❑ *Any organisation with cross-border operations is measured against all 7 principles simultaneously — in every jurisdiction*
- ❑ *One framework to internalise; multiple legal regimes to comply with*

02 Global Privacy Landscape



03 Global Data Protection Landscape

GDPR
EU — 2018
- The gold standard
- Kickstarted global movement.

CCPA
California — 2020
- Consumer rights focus
- Opt-out model

PIPL
China — 2021
- State-centric
- Strongest data localisation

LGPD
Brazil — 2020
- GDPR-inspired
- Latin America benchmark

DPDP
India — 2023+2025
- Fiduciary model
- Rules notified Nov 2025

Where the world stands on data protection regulation?

- Classifying 164 countries (including territories and free zones) on a four-tier maturity scale.
- Heavy & Robust regimes — together 86 of 164 — concentrated in EU, parts of Asia-Pacific & major economies of the Americas.
- India is rated Heavy following new legislation effective in 2026, raising compliance expectations for data flows into and out of India.

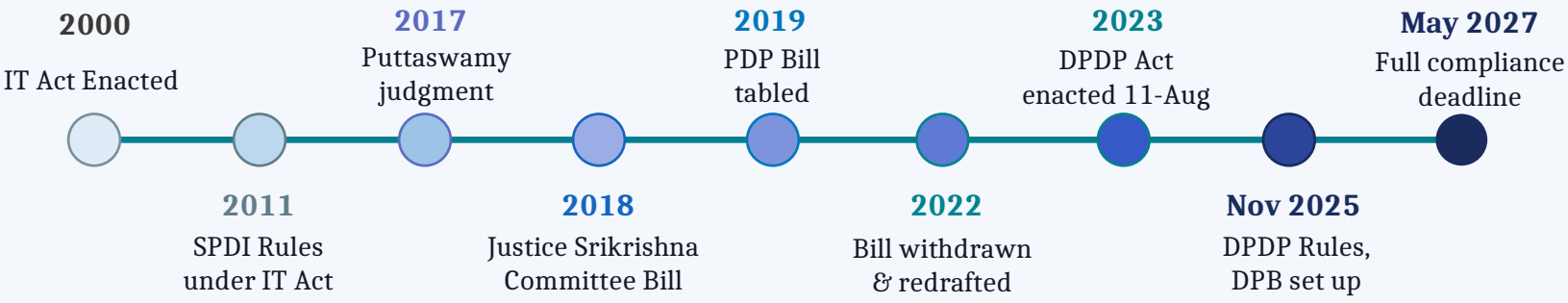
30+
HEAVY
GDPR-grade or stricter; broad enforcement

45+
ROBUST
Comprehensive law, active regulator

50+
MODERATE
Law in force; uneven enforcement

30+
LIMITED
Partial coverage or early-stage regime

04 India's Journey to DPDP — From IT Act 2000 to Rules 2025



THREE-PHASE ENFORCEMENT TIMELINE

PHASE 1 | 13 Nov 2025

Switch-On (Procedural)

Rules 1, 2 and 17–21

Effective dates, definitions, DPB establishment, administrative provisions, bar of civil court jurisdiction, conflicts with other laws.

WE ARE HERE • Board is live • Penalty framework active

PHASE 2 | 13 Nov 2026

Consent Manager Framework

Rule 4

Registration of Consent Managers as third-party intermediaries to manage Data Principal permissions and consent artefacts.

Build year — DPIA, gap assessment, RoPA, vendor reviews, training

PHASE 3 | 13 May 2027

Full Compliance

Rules 3, 5–16, 22 and 23

Notice requirements, security safeguards, breach notification, SDF obligations, Data Principal rights and grievance redressal — all enforced.

HARD DEADLINE — Penalties up to ₹250 Cr per instance

05 DPDP vs. Global Standards — Convergence & Critical Gaps

CONVERGENCE WITH GDPR

- Consent Required
- Purpose Limitation
- Data Minimisation
- Right to Correction

CRITICAL GAPS - WHAT DPDP IS MISSING vs. GLOBAL STDS

- No Automated Decision Rights
- Broad State & Union Exemptions
- No GDPR style 'Right to be Forgotten' but 'Right to Erasure'
- No Data Portability
- No Universal Privacy-by-Design Mandate
- Limited Profiling Restrictions; Stronger for Children
- DPB Independence Concerns
- No EU Adequacy — Yet

Adequacy gap costs Indian IT-BPM and pharma sectors significant compliance overhead on every EU data transfer — SCCs, Transfer Impact Assessments, BCRs. Adequacy status is a sovereign trade priority.

Key Takeaways

1. **Data is the new regulated asset**
   Treat it like cash — controlled, audited, and reported.

2. **DPDP is live — not a future project**
   Phase 1 is operational. The Board is constituted. Penalties are real. Compliance starts today.

3. **India's gap with GDPR has a cost**
   Adequacy status is a trade priority — every gap costs Indian business cross-border overhead.

Lab Systems

Data Discovery & AI for CAs

Presented by Vinay Vishwanath

Innovate
Integrate
Inspire

Lab Systems - Since 1989

Analytical Instruments to Digital Forensics

Our Journey

- 1989: Founded as an Analytical Instruments company serving FMCG, Pharma, and Forensic Labs
- 2001: Pivoted entirely to Digital Forensics - envisioning that crimes would move to computers and digital devices
- Today: India's leading Digital Forensics and GovTech AI company, operating across 17+ countries on 4 continents

90,000+
Hard Disks Analyzed

40,000+
Mobile Phones Analyzed

15+
Countries Served

35+
Years of Expertise

www.labsystems.co.in | sales@labsystems.co.in | +91 9324122665

Digital Forensic Capabilities

Trusted by Law Enforcement, Government & Enterprise

Disk Forensics

Evidence acquisition, recovery & analysis from storage media

Mobile Forensics

Smartphone data extraction, app analysis, deleted data recovery

Network Forensics

Traffic analysis, intrusion detection, log correlation

Crypto Monitoring

Blockchain tracing, wallet analysis, transaction mapping

Audio & Video

Authentication, enhancement, deepfake detection

Dark & Deep Web

Threat intelligence, monitoring, investigations

Trusted by:

CBI | Income Tax | FSLs | Ministry of External Affairs | Local Police | Private Enterprises

Why DPDP & Forensics?

Need for Privacy Enhanced Technologies

New Enterprise Risk

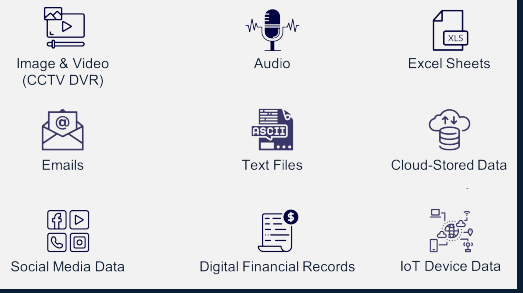
- DPDP Act 2023 mandates data fiduciary obligations
- Penalties up to INR 250 Cr for non-compliance
- Every organization collecting personal data is affected

Emerging Audit Role

- Privacy risk assessment and audit
- Data fiduciary vs processor classification
- Consent and retention practice review

Discovery Gap

- Sensitive data scattered across structured and unstructured sources
- Existing security controls are not sufficient for privacy compliance
- PII exposure often goes undetected



Diversified Tech Stack

Linux Apple Microsoft Windows android IBM ubuntu UNIX

Data Discovery: The First Step to DPDP Compliance

Structured Data

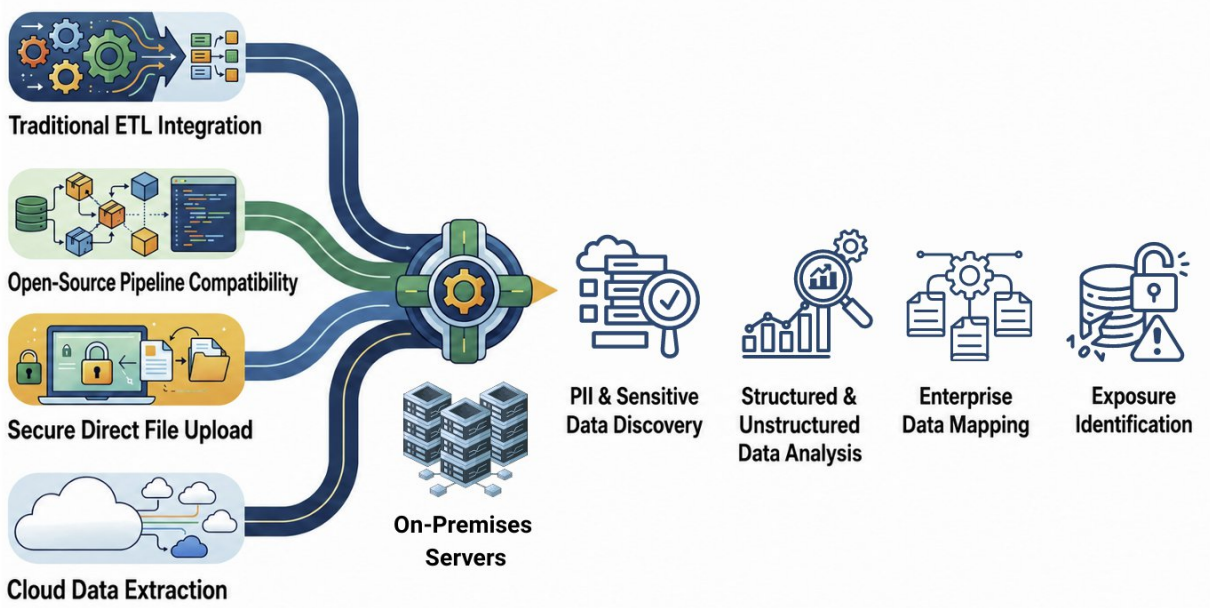
- Databases, ERP systems, CRM platforms
- Financial records, HR systems
- Customer data in spreadsheets & CSV
- API logs, transaction records
- **PII fields: Aadhaar, PAN, mobile, email, address scattered across tables**

Unstructured Data

- PDFs, Word documents, scanned forms
- Emails, contracts, legal agreements
- Images, handwritten notes (via OCR)
- Chat logs, support tickets
- **PII embedded in free text: names, addresses, health data buried in documents**

myFRT-powered Data Discovery from Structured & Unstructured Sources

Data Discovery & Privacy Assessment Workflow



Ingest

ETL, open-source pipelines, cloud extraction, direct upload

Discover

PII & sensitive data discovery across all data types via NLP + pattern matching

Assess & Analyze

DPDP gap assessment, data fiduciary/processor mapping, risk evaluation

Report

Structured compliance reports, identified gaps, risk mitigation recommendations

CHANAKAI

Private AI for Secure Organizations | Inspired by Chanakya - Built in Bharat

The power of large & small language models directly on your organization's hardware - completely offline, completely sovereign, fully under your control.

Dr. Radhakrishna Pillai

0 Cloud Calls Made

100% Data Stays On Device

Runs on Standard Laptops

20+ Open Source AI Models

Why This Matters for You & Your Clients

Organizations handling sensitive financial, legal, operational, or investigative data cannot risk exposing information to external AI services. ChanakAI eliminates this risk entirely.

ChanakAI Mini: Intelligence on Every Desk

Single Workstation, Full Solution Stack

Minimum Requirements

- 16 GB RAM, Windows 10/11
- Fully offline, air-gapped operation
- CPU: x86/64-bit architecture
- 0.5-15 GB storage per model

AI Models Included

- Gemma 4 / Qwen2.5 3B - multilingual
- Llama 3 / 3.2 3B - legal reasoning
- Mistral 7B / Phi-3.5 - fast Q&A
- 20+ additional open-source models

Built-in Use Cases for CA Practices

Document Analysis

Summarisation, validation of legal and financial documents

Legal Section ID

IPC/BNS/CrPC section identification from case files

Financial Insights

Analysis of financial statements, circulars, compliance docs

Case Timelines

Automated case file analysis and timeline generation

Supports PDF, DOCX, Excel, CSV | English & Hindi | Local OCR for scanned files

ChanakAI Max: Organisation-Wide Sovereign AI

Enterprise-grade AI on your infrastructure. No cloud. Full governance.

What ChanakAI Max Delivers

- AI command centre for entire organisation
- Role-based access control across departments
- Multi-model routing based on task type
- Document processing at scale
- Audit logs for every interaction
- REST API integration with existing systems
- GPU-accelerated performance
- Air-gapped deployment option

Designed For

- Financial & Compliance Institutions
- Enterprise Intelligence / Forensic Teams
- Government Departments
- Global Investigation Agencies
- Digital Audit & Assurance Teams

Zero data egress | Fully sovereign | Scalable multi-department deployment

Security Architecture & Compliance

Built for Regulated Environments

Air-Gapped Operation

No internet connectivity required. Zero external communication.

No Telemetry

No usage data, no analytics, no phone-home. Complete isolation.

DPDP & MeitY Aligned

Design aligned with India's data protection regulations.

Audit Logs

Every query, every interaction logged for compliance review.

Role-Based Access

Granular access control by department, role, and clearance.

On-Premise Only

Deployed on-site by our engineers. Your hardware, your control.

For CA Practices: ChanakAI enables you to offer AI-powered advisory services to clients in regulated industries without any data leaving the engagement environment.

CHANAKAI

AI AUDIT : Is Your AI aligned to your Organization?

TRIKA Framework : AI Audit on your infrastructure.

Iccha Shakti
Intent - Safety & Alignment

Sovereignty, Security & Safety

- Jailbreak Resistance Rate
- Toxicity & Harm Compliance
- Adversarial Prompt Deflection

Reliability & Alignment

- Instruction Following Accuracy
- Tone & Brand Alignment Score
- Intent Drift Detection

REASONED

Jnana Shakti
Knowledge - Integrity & Grounding

Data Integrity & Linguistic Quality

- Factual Consistency / Grounding
- PII & Data Leakage Incidence
- Hallucination Resistance Rate

Knowledge Governance

- Verbosity & Conciseness Drift
- Schema Adherence Rate
- Source Attribution Accuracy

PROBED

Kriya Shakti
Execution - Efficiency & Cost

Operational Efficiency

- P95 Latency (Response Time)
- Token Efficiency / Compression
- Cost-per-Run Inference

Execution Reliability

- Multi-Tool Orchestration Accuracy
- Error Recovery & Rollback
- Throughput Under Load

LIVE TESTED

Let's Connect

- Digital Forensics
- Data Discovery
- On-Premises AI
- AI Audits
- Training

FORENSICS

AI

PRIVACY

Lab Systems

Vinay Vishwanath
Associate Vice President
vinay@labsystems.co.in

328, Mastermind IV, Royal Palms
No.169,Aarey Milk Colony, Near
Goregaon (East),

contact@labsystems.co.in
sales@labsystems.co.in

DIGITAL PERSONAL DATA PROTECTION

NEW AVENUES

CA. UDAY KULKARNI

Dx — Digital Transformation

Integration of Digital Technologies into All Areas

DxE

Digital Transformation of Economy

DxF

Digital Transformation of Finance

DxEd

Digital Transformation of Education

DxIS

Digital Transformation of Industry & Services

DxB

Digital Transformation of Banking

DxInd

Digital Transformation of Individual

Digital Transformation of Economy

Digital Transformation of Every Sector of Economy

Digital Platforms of Economy

- Ride Sharing Aggregators — Ola, Uber
- E Commerce Platforms
- Payment Gateways

Digital Finance

- UPI
- SFMS
- SWIFT
- Cryptocurrencies
- Payment Apps

Digital Production

- IoT
- Robotic Process
- Digital Twins

Digital Business Models

- Data Analysis
- Big Data Analysis

DxInd — Digital Transformation of Individual

Physical Identity	V/s Digital Identity
Presence on Social Media	Interaction with Digital Platforms
Participation in Digital Economy	Sharing of Personal Data Details on various platforms
Sharing of Identity Data Details on various platforms	Sharing of Sensitive Data on various platforms

Protection of Citizen

- Protection of Citizen — Physically
- Protection of Citizen — Digitally
- Privacy of Citizen
- Protecting Privacy on Digital Platform
- Digital Personal Data Protection

Why Digital Personal Data Protection — For Digital Trust

DIGITAL TRUST

Protection from Misuse

Protection from AI Unethical Use

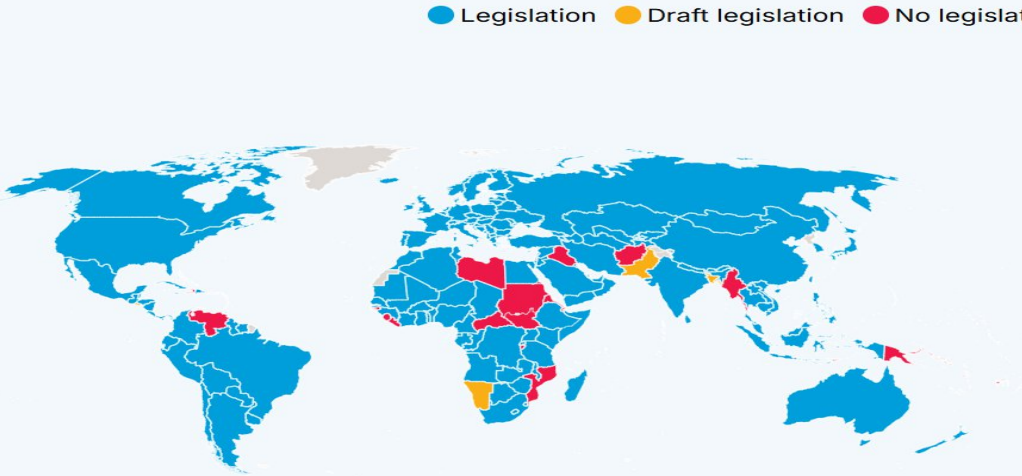
Protection from Data Theft

Protection from Data Diversion

Digital Personal Data Protection — Globally

https://unctad.org/topic/ecommerce-and-digital-economy/ecommerce-law-reform/summary-adoption-e-commerce-legislation-worldwide#

Over 140 Countries



Country group	Privacy and Data Protection
World	79%
Africa	76%
Asia and Oceania	77%
Developed countries	98%
Developing countries	73%
Landlocked developing countries	88%
Latin America and Caribbean	88%
Least developed countries	57%

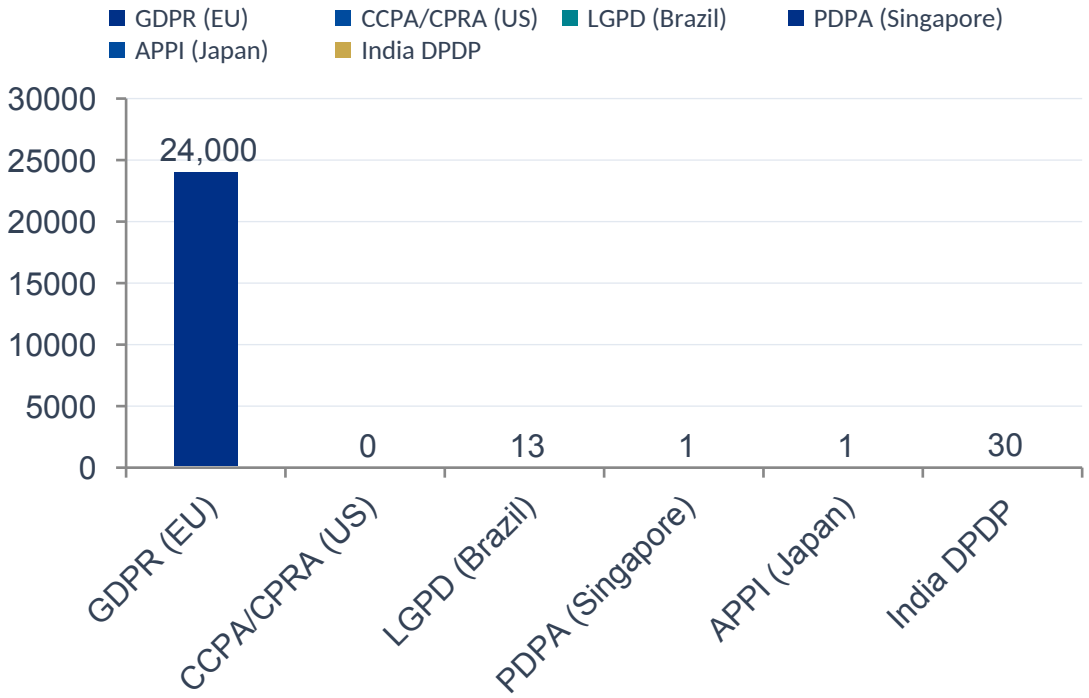
Side-by-Side Comparison

Dimension	GDPR (EU)	CCPA/CPRA (USA)	LGPD (Brazil)	PDPA (Singapore)	India DPDP 2023
Enacted	2018	2020 / 2023	2020	2012 / 2021	**2023**
Lawful Bases	6 bases incl. legitimate interests	Not applicable (opt-out model)	10 bases incl. legitimate interests	Consent + 6 other bases	**Consent + Deemed Consent (8 situations)**
Data Subject Rights	6 rights (Art. 15–21)	5+ rights (CCPA/CPRA)	8 rights (Art. 17–22)	Access, Correction, Withdrawal	**4 rights (Sections 11-13)**
Data DPO / DPA	DPO mandatory for certain entities	No formal DPO requirement	DPO mandatory	DPO not formally required	**Not required; Consent Manager concept**
Children's Data	< 16 yrs (member state can lower to 13)	< 13 yrs (COPPA); < 16 (CPRA opt-out)	< 18 yrs	< 18 yrs (advisory)	**< 18 yrs; parental consent mandatory**
Cross-Border Transfers	Adequacy / SCCs / BCRs / Derogations	No restrictions currently	Adequacy or specific mechanisms	Whitelist or contractual clauses	**Govt-notified countries / blacklist model**
Max Penalty	€20M or 4% global turnover	$7,500 per intentional violation	2% Brazil revenue (BRL 50M cap)	S$1M or 10% local turnover	**₹250 Crore per instance (≈US$30M)**
Enforcement Body	National DPAs (EDPB for consistency)	California Privacy Protection Agency	ANPD	PDPC	**Data Protection Board of India (DPBI)**

India DPDP Act vs EU GDPR: Critical Differences

Aspect	EU GDPR	India DPDP 2023	Impact
Territorial Scope	EU residents' data globally	India: digital data processed in India or for Indian principals	DPDP broadly mirrors GDPR's extra-territorial reach
Legal Bases	6 bases; Legitimate Interests is common default	Consent + 8 Deemed Consent situations; NO legitimate interests	DPDP more restrictive; consent is primary basis
Data Portability	Explicit right (Art. 20)	Not explicitly included in Act; may come via Rules	Significant gap; Indian users have fewer rights currently
Right to Object	Explicit right (Art. 21)	Not explicitly granted in Act	GDPR provides stronger objection mechanism
DPO Requirement	Mandatory for large/sensitive processing	Not required; 'Consent Manager' instead	Different compliance architecture
Cross-border Transfers	Adequacy decisions / SCCs / BCRs	Govt-notified whitelist + blacklist approach	DPDP approach is sovereign-state driven
Non-personal Data	Out of GDPR scope	Out of DPDP scope; separate bill anticipated	Gap in Indian framework for anonymised data
Enforcement	DPAs with investigative powers; class actions	DPBI — digital-first body; no class action provision	DPDP enforcement architecture still evolving

Maximum Penalty Comparison — Global Data Protection Laws



Key Penalty Notes

GDPR

€20M or 4% global turnover — highest globally; landmark fines: Meta €1.2B, Amazon €746M

India DPDP

₹250 Crore per instance; penalties are cumulative across violations; DPBI has discretion

CCPA/CPRA

$7,500 per intentional violation; private right of action for data breaches only

LGPD (Brazil)

2% of Brazilian revenue, capped at BRL 50M per violation — ANPD enforcement since 2022

Singapore PDPA

S$1M or 10% of annual local turnover — significantly enhanced post-2021 amendment

Digital Data Protection Act & CA

Applicable Across all Sectors

Significant Data Fiduciary — Large Personal Data handler

"personal data breach" means any —

- unauthorized processing of personal data, OR
- accidental disclosure, acquisition, sharing, use, alteration, destruction, OR
- loss of access to personal data,
- that compromises the confidentiality, integrity or availability of personal data;

Digital Data Protection Act & CA

Its Techno Legal Act

Protection of Digital Personal Data in Business & Commerce

Use of Digital Personal Data in Business & Commerce

Digital Personal Data Protection Act & Business Context — Assessment of Business Processes

- How the Digital Personal Data is Processed
- Need of Digital Personal Data for the Process
- Impact of Digital Personal Data Protection on Business Process

Global Requirements of Audit under Data Protection

EU GDPR	Systematic Audit of High Risk Entities
China — PIPL	Mandatory Compliance Audit under Personal Information Protection Law
Singapore — PDPC	Mandatory external audits or assessments required if organization experiences a breach or is directed by PDPC to prove accountability
Brazil — LGPD / ANPD	ANPD can require organizations to conduct audits or DPIAs to investigate data processing activities that pose significant risks to civil liberties
US State Laws	US State Specific Laws mandate regular security and privacy risk assessments

New Risk on the Enterprise Risk Radar

DATA PROTECTION NON-COMPLIANCE — A BOARDROOM AGENDA ITEM

FINANCIAL RISK

- Penalties up to ₹250 Crore per breach
- Repeat violations — cumulative penalties
- Cost of litigation & legal fees
- Remediation & forensic costs
- Insurance premium escalation

REGULATORY & LEGAL RISK

- Board inquiries & show-cause notices
- Interim orders disrupting operations
- Website/service blocking by Govt.
- Criminal liability on officers
- Cross-border transfer restrictions

OPERATIONAL RISK

- Data breach containment disruptions
- System overhaul for consent management
- Staff training & process redesign
- Vendor/processor compliance monitoring
- Technology investment requirements

REPUTATIONAL RISK

- Loss of customer trust & loyalty
- Media scrutiny on data practices
- ESG & investor confidence impact
- Brand value erosion
- Talent acquisition challenges

Emerging Role of Chartered Accountants

DPDP ACT OPENS A NEW FRONTIER OF PROFESSIONAL OPPORTUNITY FOR CAS

DATA PROTECTION AUDITOR

- Independent Data Audit (SDF mandate)
- Audit of consent mechanisms
- Review of breach notification processes
- Algorithmic audit of SDFs

DATA PROTECTION OFFICER (DPO)

- DPO appointment mandatory for SDFs
- CA's legal & compliance expertise ideal
- Board-level representation
- Point of contact for DPB

DPIA & COMPLIANCE ADVISOR

- Data Protection Impact Assessment
- Compliance gap analysis & roadmaps
- Vendor/processor due diligence
- Privacy-by-design frameworks

ASSURANCE & CERTIFICATION

- Third-party assurance reports
- Consent Manager certification
- Security safeguard attestation
- Cross-border transfer compliance

RISK ADVISORY & FINANCIAL IMPACT

- Enterprise risk assessment
- Penalty exposure quantification
- Insurance advisory on data risks
- M&A due diligence on data assets

TRAINING & CAPACITY BUILDING

- Board & C-suite sensitization
- Staff training programs
- DPDP compliance workshops
- CA firm DPDP practice setup

CA as Data Auditor — The Statutory Mandate

SECTION 10 — SIGNIFICANT DATA FIDUCIARY OBLIGATIONS CREATE A STATUTORY AUDIT REQUIREMENT

Section 10(2)(b) — A Significant Data Fiduciary shall appoint an independent data auditor to carry out data audit, who shall evaluate the compliance of the Significant Data Fiduciary in accordance with the provisions of this Act.

CONSENT AUDIT	SECURITY AUDIT	DATA LIFECYCLE AUDIT	CHILDREN'S DATA AUDIT	CROSS-BORDER AUDIT
Verify valid consent obtained for each purpose. Check withdrawal mechanism. Review Consent Manager integration.	Encryption, masking, access controls, logs. Breachnotification process. Data backup systems. 72-hour reporting window.	Purpose limitation check. Data retention schedules. Erasure on withdrawal. Third Schedule timelines. Processor agreements.	Age verification systems. Parental consent records. No behavioral tracking. No targeted advertising to minors.	Data transfer agreements. Positive list compliance. Government restrictions. SDF data localisation requirements.

Rule 13: DPIA + Audit — annually for every SDF. Report with significant observations must be submitted to the Data Protection Board.

Information Systems Audit Standard No. 430 : Audit of Digital Personal Data Protection

Contents

ICAI — Leading from Front — Certification Course

Fraud is Evolving - Are You?

Nature of Frauds

- Those where victim knowingly or innocently or out of greed or curiosity succumbs to cyber frauds –Examples :
- Responding to Phishing mails , messages,….such as
- “Your Email Have Been Awarded £109,000.00 British Pounds From COMPANY To Receive Send Your Full Name and Phone Number To Email: companyt79@gmail.com’’ or
- Business opportunities to earn huge money by becoming an agent / dealer…
- Invitations to participate in some high income yielding schemes through stock market, real estate, loan portals, ….

Blackmailing messages including digital arrest, ….

- ATTENTION

  THIS IS TO NOTIFY YOU THAT YOUR OVERDUE INHERITANCE CLAIM WITH A COMMERCIAL BANK IS TO BE RELEASED,VIA KEY TESTED TRANSFER (KT T) WIRE TRANSFER TO YOU THROUGH OUR AFFILIATE BANK IN EUROPE. IT IS PERTINENT TO NOTE THAT AN ISSUE OF THIS MAGNITUDE SHOULD HAVE COMMENCED WITH A FORMAL MEETING,BUT DUE TO THE TIME FACTOR AND THE URGENCY THIS MATTER REQUIRES,PLEASE BEAR WITH ME FOR MAKING THE INITIAL CONTACT THROUGH E-MAIL. MEAN WHILE,A MAN WITH BRITISH PASSPORT NUMBER 3028882234 CAME TO MY OFFICE FEW DAYS AGO WITH A LETTER,CLAIMING TO BE YOUR TRUE REPRESENTATIVE

  HERE ARE HIS INFORMATION BELOW:

  NAME DAVID JACKSON

  BANK NAME:CITIBANK

  BANK ADDRESS:ARIZONA, USA.

  ACCOUNT NUMBER: 6503809008.

  PLEASE,DO RECONFIRM TO THIS OFFICE ,AS A MATTER OF URGENCY IF THIS MAN IS FROM YOU,SO THAT THIS OFFICE WILL NOT BE HELD RESPONSIBLE FOR PAYING THIS INHERITANCE INTO THE WRONG ACCOUNT NAME.IF THIS MAN IS NOT YOUR REP,YOU ARE REQUESTED TO FILL AND RETURN THIS INFORMATION FOR VERIFICATION PURPOSES SO THAT YOUR INHERITANCE CLAIM VALUED US$10.5M
  DOLLARS ONLY WILL BE REMITTED INTO YOUR NOMINATED BANK ACCOUNT.

  THIS FUND IS AS A RESULT OF INHERITANCE ON YOUR BEHALF DEPOSITED BY AN AMERICAN WHO DIED IN A PLANE CRASH SOMETIME AGO.

  1. YOUR NAME:.....
  .....

  2. YOUR ADDRESS:..... .....

  3. YOUR TELEPHONE ....

  5. AGE..... .....

  6. SEX:..... .....

  7. YOUR OCCUPATION..... .....

  8. YOUR BANK DETAILS:..... .....

  AS SOON AS WE RECEIVE THE ABOVE,WE SHALL COMMENCE WITH ALL NECESSARY PROCEDURES IN OTHER TO TRANSFER THIS FUND INTO YOUR ACCOUNT THROUGH THE OFFICE OF THE DIRECTOR INTERNATIONAL REMITTANCE/FOREIGN OPERATIONS
  WHO HANDLES ALL FOREIGN INHERITANCE CLAIM.

  WE SHALL PROCEED WITH THE PAYMENT DETAILS TO THE SAID MR JACKSON,IF WE DO NOT-HEAR FROM YOU WITHIN THE NEXT THREE WORKING DAYS FROM TODAY.

  REPLY TO THIS EMAIL ADDRESS: stanbaily4@gmail.com

  BEST REGARDS.
  STANLEY BAILEY

Frauds on account of negligence of users

- User ID, Password, other credential sharing
- Not disabling Ids of ex employees and other temporary users
- Not logging out completely while using others' systems
- Not changing passwords frequently
- Obvious choices passwords - too easy to guess
- Leaving / handing over mobile, laptop, …with others giving a chance to steal data
- Entrusting sensitive, confidential accounts to others giving them a chance to make transactions in your name,…

More serious frauds

- Hacking
- Use of malwares
- Data stealing
- Encryption
- Corrupting the OS and / data base
- Spoofing identity
- The malware sits quietly in your system occupying negligible kb space which can transmit your data and enable the attacker at his convenience. The time lag before attack could be several years

Evolution of Fraud

- Today, fraud has evolved beyond physical documents and manual manipulation. It is now:
- digital,
- intelligent,
- borderless,
- automated,
- instant
- and increasingly powered by Artificial Intelligence.

- attackers can operate anonymously,
- across geographies,
- at machine speed,
- and at massive scale.

Today’s frauds are:

- identity-centric,
- platform-centric,
- and globally coordinated.

We have moved from:

- forged signatures to synthetic identities,
- fake vouchers to deepfake approvals,
- stolen passwords to session hijacking,
- and phishing emails to AI-generated personalized deception.

Fraudsters today study behavior patterns, social media presence, communication styles, and digital footprints before launching attacks.

In the digital world:

- identities can be spoofed,
- devices can be masked,
- locations can be hidden,
- and attacks can pass through multiple jurisdictions within seconds.

With technologies like:

- VPNs,
- encrypted communications,
- cryptocurrency laundering,
- botnets,
- and synthetic digital identities,
- determining “who actually committed the fraud” becomes extraordinarily difficult.

This creates a major challenge not only for law enforcement, but also for auditors, forensic investigators, compliance professionals, and boards.

The role of CA is also evolving

Today’s finance and audit professionals must understand:

- digital controls,
- cyber risk,
- data integrity,
- AI governance,
- fraud analytics,
- and technology-enabled forensic investigations.

Financial fraud and cyber fraud are no longer separate domains.

Increasingly:

- accounting controls,
- cybersecurity controls,
- identity management,
- and governance frameworks

must work together.

Risk of CA is increasing

- You certify the adequacy of Internal Financial Controls.

  Any Cyber or other fraud can easily be attributed to failure of IFCs.
- Does the scope of your normal audit include and is capable of unearthing layered transactions?
- Role and review by CA has gone beyond certifying the numbers.
- You are supposed to be reviewing the various risks which include the frauds

Fraud is Evolving-Are You?

Sahil Malik

Chief General Manager, Securities and Exchange Board of India

The Fraud Reality: What We Keep Missing

The Fraud Reality: What We Keep Missing

Warning signs existed

...but were ignored

Transactions were visible

...but unchallenged

Governance was weak

...but unquestioned

Skepticism eroded

...gradually

"Every major fraud was once a small ignored anomaly."

The New Fraud Architecture: From Transaction to Narrative Fraud

Old Fraud

- Simple transaction manipulation
- Arithmetic inaccuracies
- Obvious falsification
- Isolated incidents

Modern Fraud

- Engineered growth stories
- Fabricated valuation narratives
- Investor sentiment manipulation
- Governance appearance – compliant on paper

What CAs Must Now Evaluate:

Economic Substance

Behavioural Patterns

Governance Quality

Technology Vulnerabilities

Management Intent

"Complexity is often the preferred hiding place of manipulation."

Learnings from SEBI CFID Orders

Revenue Recognition Fraud: The Illusion of Growth

Fraud Type 1 of 5

Common Structures

- Fictitious sales & shell customers
- Circular transactions & round-tripping
- Channel stuffing
- Premature revenue recognition
- Post-period reversals

🚩 Red Flags

- Revenue growth without matching cash flow
- Rising receivables despite profitability
- Quarter-end sales spikes
- Concentration of sales among new entities
- Aggressive pressure to 'meet numbers'
- Resistance to customer confirmations

✔ Preventive Measures

- Customer-network mapping & independent confirmations
- GST and e-way bill reconciliation
- Receivable ageing analytics
- Post-period reversal testing
- Excessive top-side journal entry monitoring

"Cash flow usually reveals what profits attempt to conceal."

Case Vignettes: Revenue Fraud in Practice

Case 1: Pharmaceutical Company

- Inflated sales and profits through fictitious purchases with controlled entities
- Multiple sets of financial statements created for FY 2010-11 to 2012-13
- Fabricated figures signed off by statutory auditors
- Objective: Mislead stakeholders with fabricated financial data

Case 2: Real Estate Development Company

- Revenue from flat/land sales and interest expenses overstated
- Assets (PPE, trade receivables) deliberately misclassified
- Financial statements manipulated to disguise related-party exposure
- Inflated asset quality to misrepresent financial health

Lesson: Warning signs were present — but professional skepticism was absent.

Impairment Manipulation: Concealment & Diversion

Impairment Manipulation: Concealment & Diversion

Fraud Type 2 of 5

Two Types of Impairment Fraud

Type 1: Non-Recognition of Impairment

- Avoid impairment to sustain valuations
- Preserve profitability & market confidence
- Prevent covenant breaches
- Stressed subsidiaries carried at inflated values
- Large goodwill despite deteriorating operations

Type 2: Fraudulent Impairment for Diversion

- Impairment used to suppress asset values
- Facilitate undervalued transfers to related parties
- Justify write-offs and conceal diversion
- Promoter-linked restructuring at depressed prices
- Assets suddenly impaired before restructuring

Preventive Measures

- Independent valuation review & fairness opinions for material write-downs
- Reverse sensitivity testing & industry benchmarking
- Forensic review of impairment-linked restructuring
- Audit committee review of valuation assumptions

"A sudden destruction of value on paper may sometimes precede a transfer of value in reality."

Valuation Fraud: Valuation as a Vehicle of Deception

Fraud Type 3 of 5

Especially Prevalent In:

- **Startups**
- **PE Transactions**
- **Slump Sales**
- **Related-Party Deals**
- **Intangible Valuation**
- **Restructuring**

Type 1: Overvaluation

- Attract investors & inflate market cap
- Aggressive DCF assumptions
- Unrealistic growth projections
- Repeated upward revisions
- Promoter-linked valuation influence

Type 2: Undervaluation

- Facilitate promoter-linked acquisitions
- Transfer value from public shareholders
- Enable restructuring at depressed prices
- Suppress tax exposure
- Assets impaired before distressed sale

Case: SEBI blocked ₹95 crore slump sale of core assets to promoter-group entity (Par Drugs & Chemicals Ltd) – alleged severe undervaluation.

Substance Over Form Frauds: Legally Compliant, Economically Misleading

Fraud Type 4 of 5

"Economic substance must prevail over legal architecture."

Common Structures:

- Off-balance-sheet arrangements
- Related-party camouflage
- Layered SPV structures
- Circular fund routing
- Hidden liabilities & guarantees

Red Flags:

- Excessive legal complexity
- Transactions lacking commercial rationale
- Repeated fund routing through entities
- Unusual year-end restructuring
- High volume of adjusting journal entries

Case: Home Finance Company

- Excessive general-purpose corporate loans to financially weak, newly incorporated, and promoter-associated entities
- Fabricated agreements and circular fund flows disguised fund diversion as routine financial transactions

Preventive Measures: Beneficial ownership mapping | Forensic fund-flow analysis | Related-party clustering | Transaction substance review

Governance Failure: The Root Cause Behind Most Frauds

Fraud Type 5 of 5

Most major frauds had controls, audit committees, and auditors — yet failed. Why?

Management Override

Controls bypassed by top leadership with concentrated authority

Dissent Became Unsafe

Challenge culture suppressed; fear of retaliation for raising concerns

Ceremonial Governance

Boards and committees existed but did not genuinely scrutinize

Skepticism Weakened

Professional skepticism gave way to trust, optimism, and silence

Case: Entertainment Enterprises

- Promoter issued ₹200 crore fixed deposit guarantee letter without Board approval
- Material related-party transactions not disclosed; assets appropriated by a connected financial institution

"The greatest vulnerability in any control framework is concentrated authority without accountability."

Master Red Flag Matrix: Key Warning Signals Across Fraud Types

Fraud Type	Financial Indicators	Governance Indicators
Revenue Fraud	Revenue ↑ without cash flow; Rising receivables; Q-end spikes	Pressure to meet numbers; Resistance to confirmations
Impairment Fraud	Sudden large write-downs; Impairment before restructuring	Valuation by connected parties; Weak audit committee
Valuation Fraud	Aggressive DCF; Unrealistic projections; Valuation disconnected from industry	No competitive bidding; Related-party valuers
Substance Fraud	Excessive legal complexity; Circular fund routing; High journal entries	Repeated year-end restructuring; Beneficial ownership opaque
Governance Failure	Unexplained transactions; Undisclosed guarantees	Promoter dominance; Board unable to challenge management

The presence of multiple red flags from different categories significantly elevates fraud risk assessment.

Suggestions for the Profession: Redesigning Governance Architecture (1/2)

01 Fraud-Risk Workshops for Audit Committees

02 Mandatory Economic Substance Review

03 Independent Review of Related-Party Transactions

"An informed audit committee is one of the strongest anti-fraud controls in any organization."

Suggestions for the Profession: Redesigning Governance Architecture (2/2)

04 ERP-Level Hard Controls for Sensitive Transactions

05 Open-Source Intelligence (OSINT) in Audit Planning

06 Dual Independent Valuation Opinions

"Fraud leaves behavioural footprints long before it leaves accounting evidence."

Behavioural Nudges & Ethical Architecture in Fraud Prevention

A 'nudge' = behavioural intervention to influence ethical decision-making without coercion.

1. Ethical Declaration Before Sensitive Transactions

Senior officials digitally confirm: 'This transaction has genuine commercial substance and does not involve concealment or conflict of interest.' Creates psychological accountability.

2. Behavioural Warning Prompts in ERP

ERP displays: 'This transaction is high fraud-risk category' or 'This journal entry bypasses approval hierarchy.' Promotes pause-based decision making.

3. Fraud-Awareness Certification by Business Heads

Quarterly certifications: no undisclosed RPTs, no side agreements, no artificial revenue structures. Expands accountability beyond finance.

4. Ethical Climate Surveys & Red-Flag Escalation

Anonymous surveys evaluate: fear of retaliation, pressure to meet targets, transparency. Direct escalation channels for suspicious transactions without fear.

"Fraud risk is often cultural long before it becomes financial."

Ethical Perspective: The Core of Our Profession

Fraud prevention is not merely a technical exercise — it is an ethical responsibility.

The Ethical Challenge Before the Profession

- Normalization of aggressive conduct
- Pressure-driven silence in organizations
- Gradual ethical compromise
- Rationalization of exceptions and overrides
- One ignored exception → one massive fraud

The Real Defence Lies In:

- Professional skepticism — always question
- Ethical courage — speak up against pressure
- Governance integrity — substance over form
- Willingness to question economic reality
- Convergence of vigilance & forensic intelligence

How Fraud Begins — The Path of Small Compromises:

One ignored exception → One undocumented adjustment → One pressured approval → One rationalized override → FRAUD

Technology identifies anomalies. Controls reduce opportunities. But the first line of defence is professional integrity.

The real defence lies in the convergence of vigilance, forensic intelligence, governance integrity, and professional courage.

Because every financial system survives not merely on regulation — but on TRUST.

Fraud is Evolving - Are You?

Nature of Frauds

- Those where victim knowingly or innocently or out of greed or curiosity succumbs to cyber frauds –Examples :
- Responding to Phishing mails , messages,….such as
- “Your Email Have Been Awarded £109,000.00 British Pounds From COMPANY To Receive Send Your Full Name and Phone Number To Email: companyt79@gmail.com’’ or
- Business opportunities to earn huge money by becoming an agent / dealer…
- Invitations to participate in some high income yielding schemes through stock market, real estate, loan portals, ….

Blackmailing messages including digital arrest, ….

- ATTENTION

  THIS IS TO NOTIFY YOU THAT YOUR OVERDUE INHERITANCE CLAIM WITH A COMMERCIAL BANK IS TO BE RELEASED,VIA KEY TESTED TRANSFER (KT T) WIRE TRANSFER TO YOU THROUGH OUR AFFILIATE BANK IN EUROPE. IT IS PERTINENT TO NOTE THAT AN ISSUE OF THIS MAGNITUDE SHOULD HAVE COMMENCED WITH A FORMAL MEETING,BUT DUE TO THE TIME FACTOR AND THE URGENCY THIS MATTER REQUIRES,PLEASE BEAR WITH ME FOR MAKING THE INITIAL CONTACT THROUGH E-MAIL. MEAN WHILE,A MAN WITH BRITISH PASSPORT NUMBER 3028882234 CAME TO MY OFFICE FEW DAYS AGO WITH A LETTER,CLAIMING TO BE YOUR TRUE REPRESENTATIVE

  HERE ARE HIS INFORMATION BELOW:

  NAME DAVID JACKSON

  BANK NAME:CITIBANK

  BANK ADDRESS:ARIZONA, USA.

  ACCOUNT NUMBER: 6503809008.

  PLEASE,DO RECONFIRM TO THIS OFFICE ,AS A MATTER OF URGENCY IF THIS MAN IS FROM YOU,SO THAT THIS OFFICE WILL NOT BE HELD RESPONSIBLE FOR PAYING THIS INHERITANCE INTO THE WRONG ACCOUNT NAME.IF THIS MAN IS NOT YOUR REP,YOU ARE REQUESTED TO FILL AND RETURN THIS INFORMATION FOR VERIFICATION PURPOSES SO THAT YOUR INHERITANCE CLAIM VALUED US$10.5M
  DOLLARS ONLY WILL BE REMITTED INTO YOUR NOMINATED BANK ACCOUNT.

  THIS FUND IS AS A RESULT OF INHERITANCE ON YOUR BEHALF DEPOSITED BY AN AMERICAN WHO DIED IN A PLANE CRASH SOMETIME AGO.

  1. YOUR NAME:.....
  .....

  2. YOUR ADDRESS:..... .....

  3. YOUR TELEPHONE ....

  5. AGE..... .....

  6. SEX:..... .....

  7. YOUR OCCUPATION..... .....

  8. YOUR BANK DETAILS:..... .....

  AS SOON AS WE RECEIVE THE ABOVE,WE SHALL COMMENCE WITH ALL NECESSARY PROCEDURES IN OTHER TO TRANSFER THIS FUND INTO YOUR ACCOUNT THROUGH THE OFFICE OF THE DIRECTOR INTERNATIONAL REMITTANCE/FOREIGN OPERATIONS
  WHO HANDLES ALL FOREIGN INHERITANCE CLAIM.

  WE SHALL PROCEED WITH THE PAYMENT DETAILS TO THE SAID MR JACKSON,IF WE DO NOT-HEAR FROM YOU WITHIN THE NEXT THREE WORKING DAYS FROM TODAY.

  REPLY TO THIS EMAIL ADDRESS: stanbaily4@gmail.com

  BEST REGARDS.
  STANLEY BAILEY

Frauds on account of negligence of users

- User ID, Password, other credential sharing
- Not disabling Ids of ex employees and other temporary users
- Not logging out completely while using others' systems
- Not changing passwords frequently
- Obvious choices passwords - too easy to guess
- Leaving / handing over mobile, laptop, …with others giving a chance to steal data
- Entrusting sensitive, confidential accounts to others giving them a chance to make transactions in your name,…

More serious frauds

- Hacking
- Use of malwares
- Data stealing
- Encryption
- Corrupting the OS and / data base
- Spoofing identity
- The malware sits quietly in your system occupying negligible kb space which can transmit your data and enable the attacker at his convenience. The time lag before attack could be several years

Evolution of Fraud

- Today, fraud has evolved beyond physical documents and manual manipulation. It is now:
- digital,
- intelligent,
- borderless,
- automated,
- instant
- and increasingly powered by Artificial Intelligence.

- attackers can operate anonymously,
- across geographies,
- at machine speed,
- and at massive scale.

Today’s frauds are:

- identity-centric,
- platform-centric,
- and globally coordinated.

We have moved from:

- forged signatures to synthetic identities,
- fake vouchers to deepfake approvals,
- stolen passwords to session hijacking,
- and phishing emails to AI-generated personalized deception.

Fraudsters today study behavior patterns, social media presence, communication styles, and digital footprints before launching attacks.

In the digital world:

- identities can be spoofed,
- devices can be masked,
- locations can be hidden,
- and attacks can pass through multiple jurisdictions within seconds.

With technologies like:

- VPNs,
- encrypted communications,
- cryptocurrency laundering,
- botnets,
- and synthetic digital identities,
- determining “who actually committed the fraud” becomes extraordinarily difficult.

This creates a major challenge not only for law enforcement, but also for auditors, forensic investigators, compliance professionals, and boards.

The role of CA is also evolving

Today’s finance and audit professionals must understand:

- digital controls,
- cyber risk,
- data integrity,
- AI governance,
- fraud analytics,
- and technology-enabled forensic investigations.

Financial fraud and cyber fraud are no longer separate domains.

Increasingly:

- accounting controls,
- cybersecurity controls,
- identity management,
- and governance frameworks

must work together.

Risk of CA is increasing

- You certify the adequacy of Internal Financial Controls.

  Any Cyber or other fraud can easily be attributed to failure of IFCs.
- Does the scope of your normal audit include and is capable of unearthing layered transactions?
- Role and review by CA has gone beyond certifying the numbers.
- You are supposed to be reviewing the various risks which include the frauds