CYBER & FINANCIAL CRIMES
IN INDIA

Deepfakes, Digital Trials, Crypto Frauds

& the Widening Threat Landscape

Sai Sri

SP, Cybercrimes,

Telangana Cyber Security Bureau

India's Digital Boom - A Double-Edged Sword

- India has one of the fastest growing digital banking & UPI ecosystems globally
- Rapid digitisation has massively expanded the attack surface for cybercriminals
- BFSI sector remains the #1 target due to real-time financial transactions
- Frauds now target customer trust & psychology - not just systems and networks

What Are We Facing Today?

AI-Based Frauds

Deepfake scams & synthetic identities

UPI & QR Frauds

Payment manipulation & fake QR

Phishing & Vishing

Fake customer care, smishing

Crypto Scams

Money laundering & crypto fraud

Digital Arrests

Fake officer video-call coercion

Ransomware

Bank & BFSI infrastructure attacks

EMERGING THREAT

Deepfakes - The New Face of Impersonation

- AI-generated voices & videos used to impersonate bank officials, police & family
- Victims convinced to transfer funds through fabricated visual authority
- Deployed in fake investment schemes and digital arrest scams
- Near-impossible to detect without dedicated forensic tools
- LEAs face evidential challenges - digital forgery is increasingly indistinguishable

⚠ **India reported a 300% surge in deepfake fraud cases between 2023–2025**

⚠ HIGH ALERT FRAUD TYPE

Digital Arrests - Psychological Warfare on Citizens

HOW IT WORKS

1. Fraudster poses as CBI / ED / Police / Customs officer
2. Victim kept on live video call under fake 'arrest'
3. Accused of fake crimes - NDPS, money laundering, smuggling
4. Coerced into immediate large fund transfers

PRIMARY TARGETS

- Elderly citizens
- Working professionals
- Students & NRIs
- Business owners

Cryptocurrency - The New Frontier of Financial Crime

Anonymous Wallets

P2P transactions mask the true identity of fraudsters

Rapid Layering

Funds moved instantly across multiple platforms & wallets

Money Laundering

Crypto used to integrate proceeds of crime into legal economy

Terror Financing

Cross-border crypto transfers fund illegal activities

Why Is It Hard to Catch Cybercriminals?

Fake Identities & VPNs

Criminals use mule accounts, VPNs and anonymisation tools

Cross-Border Jurisdiction

Foreign servers and international financial channels complicate investigation

MLAT Delays

Obtaining digital evidence from foreign jurisdictions takes months

Rapid Fund Movement

Money laundered through multiple accounts before freezing is possible

AI / Deepfake Sophistication

Impersonation tools outpace current forensic detection capabilities

Low Public Awareness

Delayed reporting leads to greater financial losses and cold trails

How the BFSI Sector Is Responding

AI-Driven Fraud Detection

Zero Trust Security Model

Behavioural Biometrics

Anti-Deepfake Video-KYC

Real-Time Account Freeze

Cyber Resilience Drills

Regulatory & Compliance Landscape

- RBI mandates on fraud reporting timelines for all scheduled banks
- Mandatory cyber audits for all BFSI entities annually
- Third-party and vendor risk management requirements strengthened
- Digital payment security norms upgraded under DPSS framework
- Coordinated mechanism between LEAs, RBI, CERT-In and NPCI

Building Cyber Resilience - Collectively

01

Real-Time Threat Intelligence Sharing

Between LEAs, banks, CERT-In and NPCI

02

Stronger LEA–Bank–Tech Collaboration

Joint ops, dedicated cyber cells, fast FIR registration

03

Public Awareness Campaigns

Targeted outreach to elderly, rural and high-risk groups

04

Faster MLAT & International Cooperation

Bilateral agreements to accelerate evidence sharing

05

Proactive Cyber Frameworks

Move from reactive response to predictive prevention

Thank you!

"Cybersecurity is a Shared Responsibility"

Cybercrime is no longer just a digital threat - it is an economic, psychological, and national security challenge. Resilience, awareness and vigilance remain our strongest defence against evolving cyber and financial crimes.

Cybersecurity & Resilience Trends (BFSI)

- A Practitioner's perspective

Digital Transformation (Dx) Finance Summit 2026

Rajesh Thapar

CISO,

National Stock Exchange of India Ltd

Cyber is a Asymmetric Battlefield

Economic Asymmetry (Cost to Kill)

1. **The Attacker's Budget:** "R&D" is crowd-sourced. Use stolen infra to attack yours. Light, agile, $50 tools, *"Needs to be right once.*
2. **Cyber Budget:** 50+ security tools, $5M budget, *"Needs to be right 100% of the time*
3. **The ROI Gap**: An attacker's ROI is calculated in Bitcoin; and Cyber ROI is "nothing happened today" (which is hard to sell to a CFO).

For every $1 an attacker spends on a polymorphic script, a CISO spends $1,000 on licensing, integration, training, and monitoring.

Temporal Asymmetry (Clock)

1. **"Dwell Time" :** Attackers move in silence and wait for the "perfect storm" (e.g., a holiday weekend or a merger).
2. **The Defender's Race:** The Cyber Team is always reactive to the "Alert."
3. **Data Point: A**verage time to identify and contain a cross environment breach is 241 days – IBM Cost of a Data Breach Report 2025

Cognitive Asymmetry (Human Factor)

1. **The "Script" vs. the "Social":** We spend millions on AI-driven firewalls, but the attacker wins with a Zero cost phone call pretending to be "Jimmy from IT."
2. **The AI Force Multiplier:** Generative AI has removed the "tells" of phishing (bad grammar, weird formatting). Now, the asymmetry is perfect: a low-skill attacker can generate high-skill deception.

The math is broken. We don't need a bigger shield; we need a different game."

Digital Transformation Security Considerations

Must Assure: INTEGRITY | TRUST | RELIABILITY | SECURITY | PRIVACY

Enablers: Tech Innovation | Financial Inclusion | Regulations | Data Explosion | Interconnected

Organizations

01 Competitiveness and reduced time to market

Competitiveness and reduced time to market

02 Convenience vs security

Expectations - Convenience vs security

03 Regulations and Legislations

Regulations and Legislations

04 Upstream and Downstream impact

Upstream and Downstream impact

05 Increasing Monetary & Nonmonetary loss

Increasing Monetary & Nonmonetary loss

06 Tech is helping both Attacker and Defender.

Tech is helping both Attacker and Defender.

07 Cyber has evolved to be a Business Risk

Cyber has evolved to be a Business Risk

Individuals

Human element
- Greed,
- Error
- Ignorance
- Fear

Reachability

Compromised Mobile devices

Identity theft

Easily Trust the perpetrator

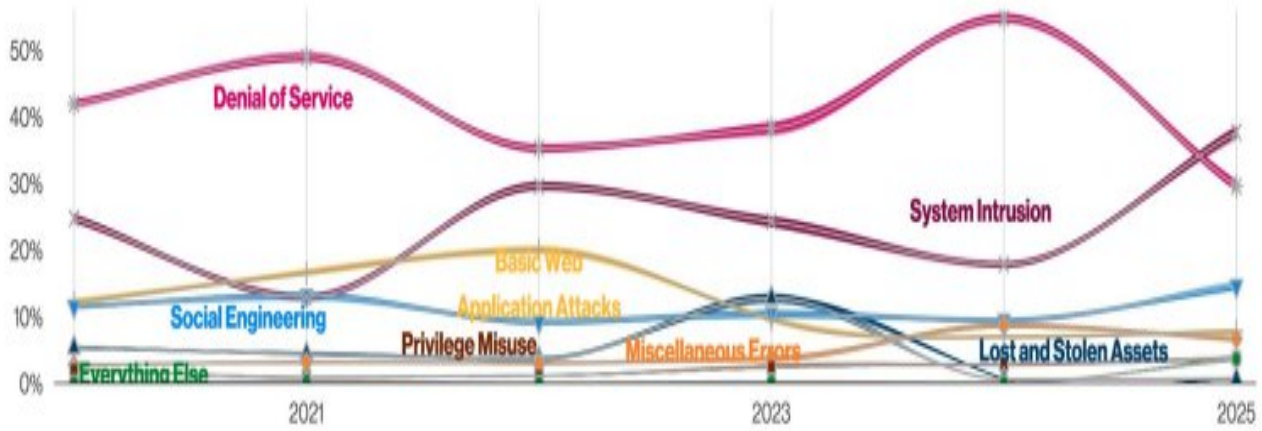
Ease of Impersonation –
- Deepfake
- Social media handle
- Fake Mobile app

Common and Trivial passwords and PIN

Jurisdiction / boundaryless security

Ease of attack – Tools and exploit availability, low cost, low expertise, market place

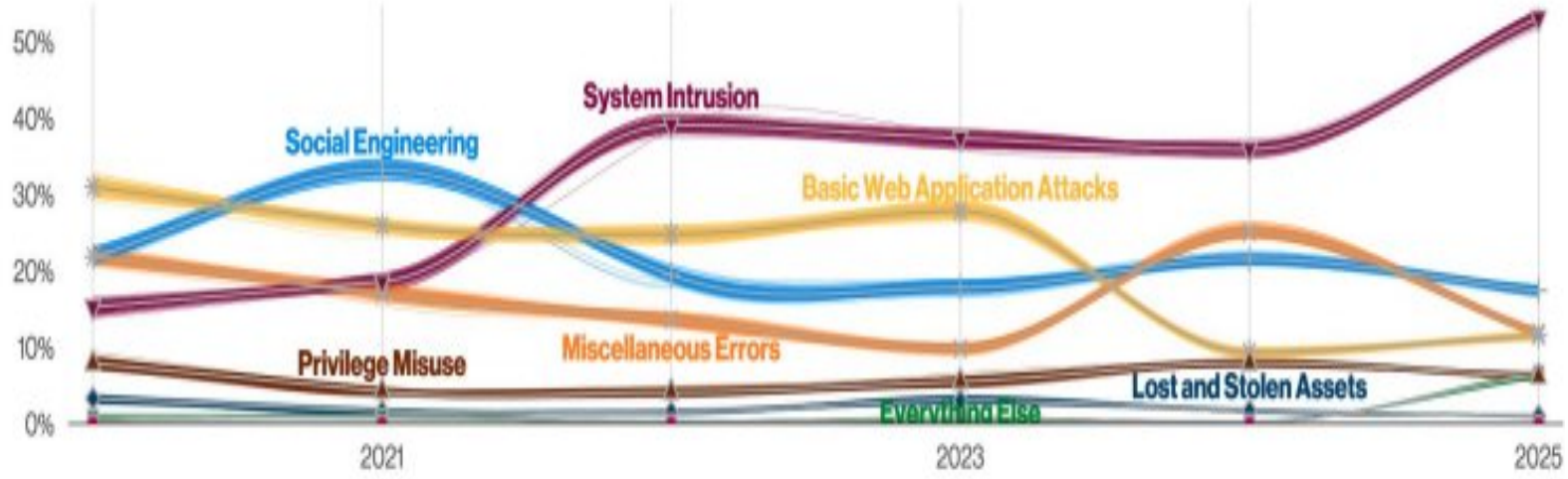
Global Report : Attack Vector Patterns



Security Incidents

Top Attacks targeting BFSI

- DDoS
- Ransomware
- Data based attacks
- Application attacks
- Supply Chain
- AI-based

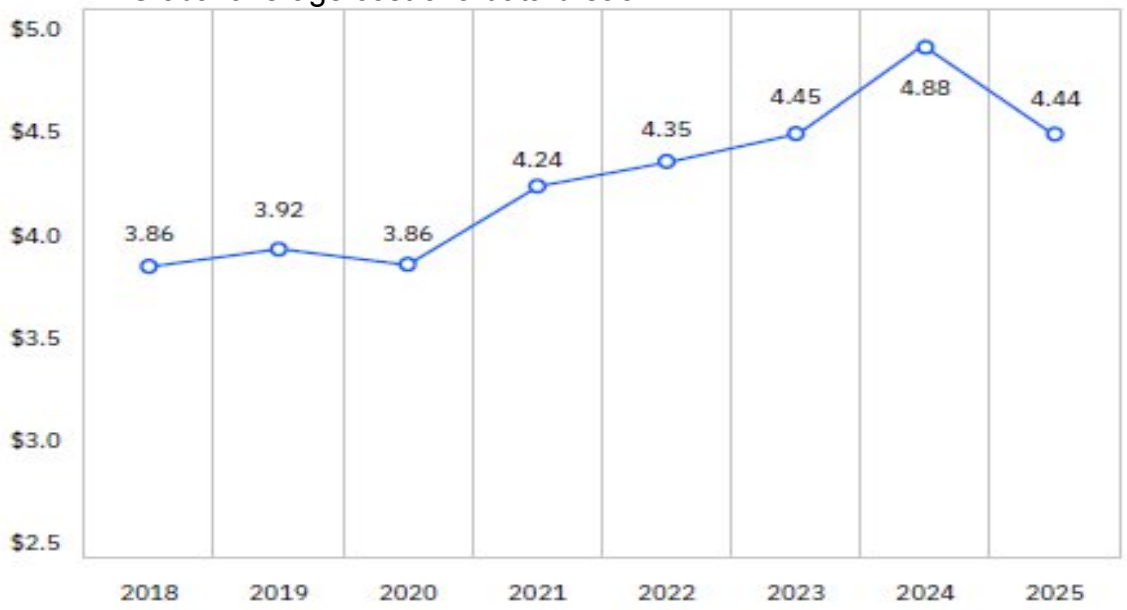


Security breaches

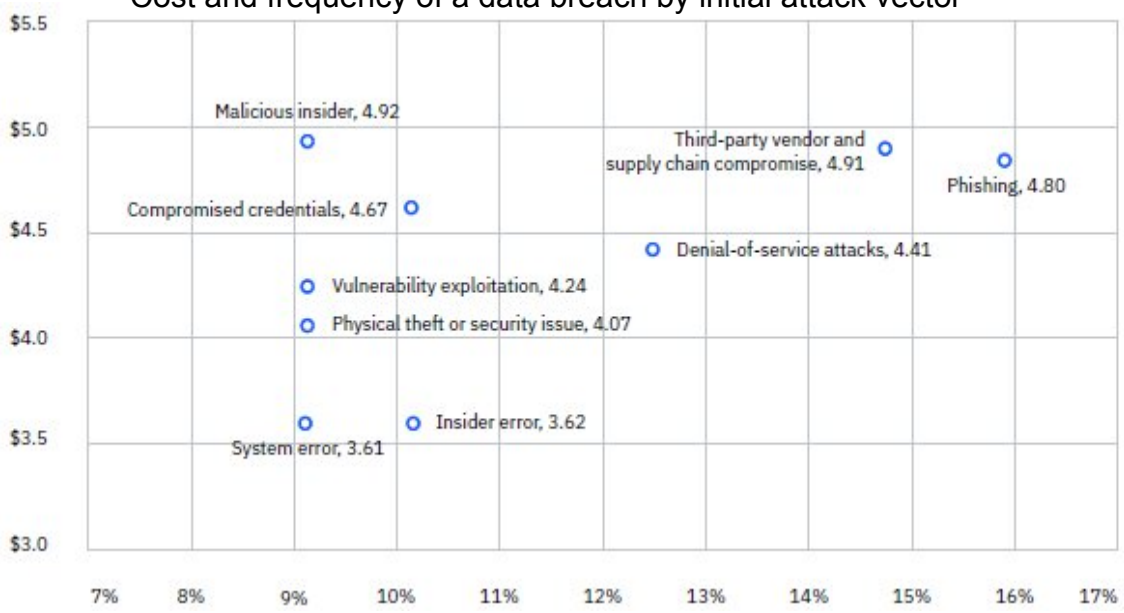
Source : 2025 Verizon DBIR

IBM Cost of Cyber Breach Study 2025 (Ponemon Institute)

Global average cost of a data breach



Cost and frequency of a data breach by initial attack vector



Key Insights	
USD 4.44 M – Global (2024-USD 4.88M) **USD 2.51M – India (2024-USD 2.35M)**	• **USA Tops ($10.22M) and India – 14th (2024-15th Rank)** • **Financial Sector Avg : USD 5.56M (2024-USD 6.08M) ;Healthcare USD 7.42 (2024- USD 9.77M)**
Only 50% breaches detected by internal tools and security teams	**In 2024, only 42% breaches were detected.**
241 days (2024-258 days) **Average time to Identify and contain a data breach**	• **181 Days to Identify a breach** • **60 Days to Contain** data breach

Summary

- ✓ Globally, 9% decrease (YoY) in average costs of a data breach.
- ✓ Malicious insider attacks resulted in the highest average breach costs among initial threat vectors: USD 4.92 M.
- ✓ Third-party vendor and supply chain compromise attacks took the longest to identify and contain (Avg-267 days)
- ✓ AI & automation enabled organizations' security and security service teams on faster identification and containment of breaches.

Source : IBM Cost of Cyber Breach Study 2025(Ponemon Institute)

Evolution of Cyber Attributes

	Past	Present	Future
Concerns to address	**GOVERN & PROTECT** • Phishing • Perimeter • Hacking/ Malware • 3rd party risks	**DETECT & RESPOND** • Supply Chain attacks • Visibility gaps • Alert fatigue • Talent shortage • Shadow IT Manage Team's Stress levels	**RESILIENCE** • Contribute to Biz • Support emerging tech • AI driven threats (+ Shadow AI) • Geopolitical tensions
Skills	• 'Fighter' • Tech Specialist • GRC • Vulnerability assessor	• Risk and threat Modeling • Executive Communication • Negotiator • Stakeholder management	• Articulation ('Story Teller') • Safe use of Emerging Tech • Ethics and Digital Trust • Geo-cyber risks
Risk Appetite	• Adhoc • Compliance driven • Reactive • Zero issues target	• Formal and Board approved • Business Aligned • Managed Risk (Balanced)	• Adaptive and predictive with real time adjustments • Integrated with ERM • Value-Driven Risk (Strategic)

Evolution of Cyber Attributes

	Past	Present	Future
Adversaries	Script Kiddies	Ransomware Cartels & Nation State	Anyone with access to AI
Visibility	Significant Unknowns	• Dynamic Attack Surface • Attacker profiles • Threat Hunting • 3V event syndrome	• AI and Data driven insights • Near Zero unknowns
Priorities	Castle - The Corporate Network Hardshell of perimeter	• Manage the "Blast Radius • Data Centric security • Automation • Secure by Design Protect “Value Chain" (Vendors, APIs, Cloud)	Ability to absorb a shock and keep running without losing customer faith. • Simulations • Continuous Cyber Assurance Protect "Truth" (Deepfakes, AI hallucinations, Data Poisoning, Privacy)

Transformation of Cyber in BFSI

Cyber of the past (Cyber Security)

Lead by Person with tech know how to implement controls and prevent cyber attacks

- **Protect** and **Monitor**
- **Avoid Risks** – perceived as 'NO' man
- **Tech Aligned Controls**
- **Toll Gate** Keeper
- **Secure by Design**
- **Compliance to ISO27001** & similar standards
- **Security** is **IT Risk**
- **Limited interactions** with CEO / Board
- **Cyber Awareness**
- **Risk Assessments and Audits**

Next Gen Cyber (Cyber Resilience)

+ Business know how to prevent and manage cyber risks and attacks

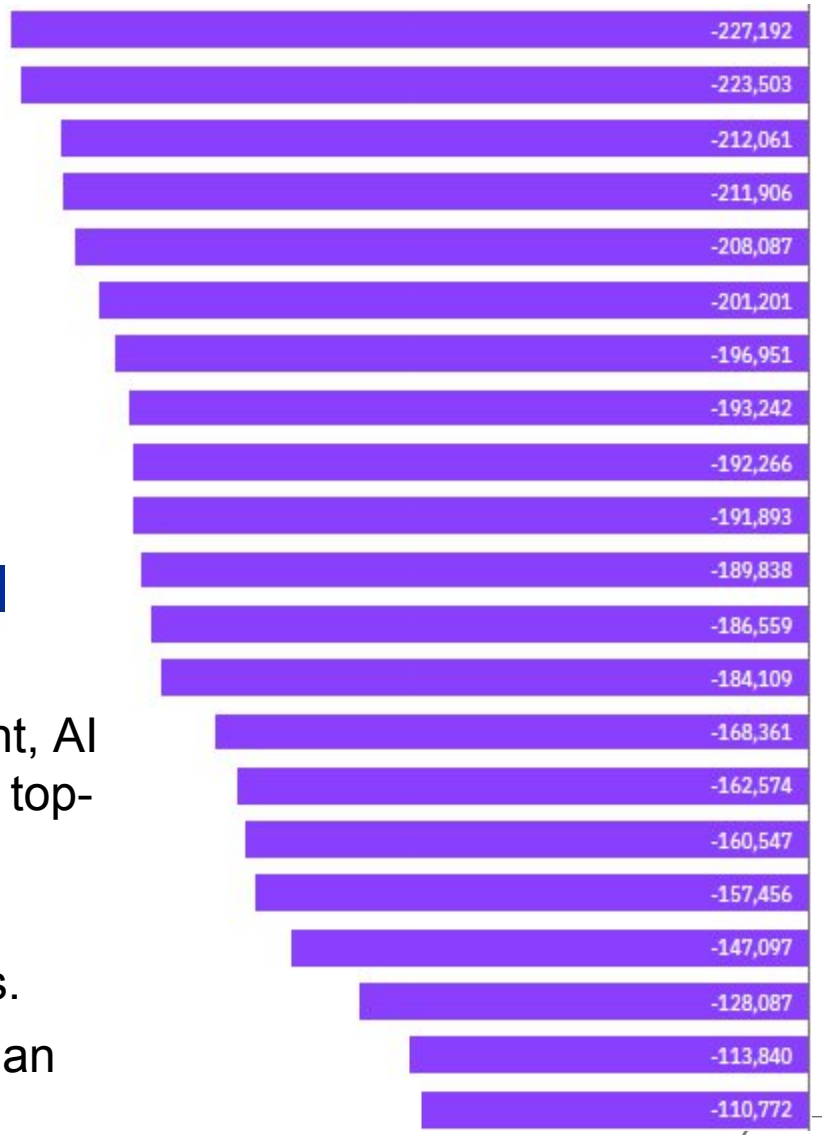
- **+ Cyber Resilience**
- **+ Assume Breach**
- **+ Manage Risks** – Solution orientation
- **+ Business Aligned Cyber Strategy**
- **+ Resilience by Design**
- **+ Security is Business Risk**
- **Regular interaction** with **CEO & Board**
- **Cyber Risk Culture**
- **Attack Simulation and resilience testing**

Reactive **Preemptive** **Proactive**

Factors impacting the cost of breach

Key factors resulting in Increase

Key factors resulting in Decrease



Key Factors 2025	KF Prev
DevSecOps approach	7
AI-driven and ML-driven	2
Security analytics or SIEM	3
Threat intelligence	6
Encryption	5
SOAR tools	11
Quantum security tools	-
Proactive threat hunting	10
Employee training	1
AI governance technologies	-
IAM	9
Machine learning SecOps	-
Offensive security testing	13
EDR tools	15
Gen AI security tools	16
Attack surface management	-
Data security and protection	17
AI governance policies	-
MSSP	20
CISO appointed	19
Board-level oversight	18

Summary

- ✓ DevSecOps approach to software development, AI & ML insights and having a SIEM rounded the top-three controls.
- ✓ Security system complexity and supply chain breaches continue to challenge security teams.
- ✓ Shadow AI presence within an organization is an added blind spot.

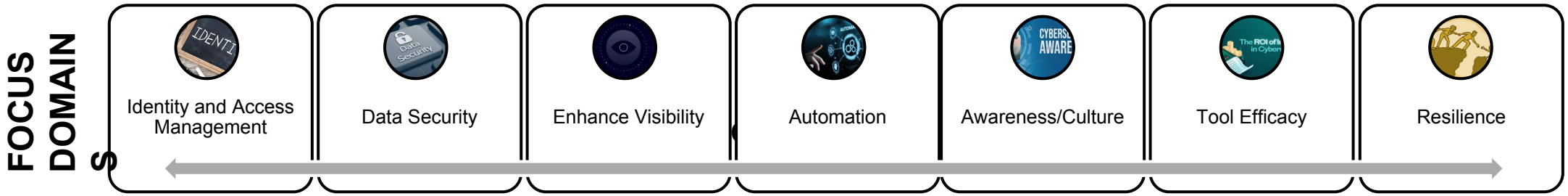
Source : IBM Cost of Cyber Breach Study 2025(Ponemon Institute)

Cyber Resilience – Key trends

Goal	ANTICIPATE	WITHSTAND	RECOVER	ADAPT
What it means ?	Maintain awareness of threats; deter avoid and prevent before they materialize	Absorb attacks and continue critical operations during adverse events	Restore systems, services and data with minimal disruption after an incident	Learn from Incidents and evolve defenses to handle future threats
Key trends	• Risk Assessments • Multi-layer Architecture • Continuous user awareness • Threat Intelligence integration	AI augmented SOC XDR	• BCP with Immutable backups • Isolated Recovery Environment	Detailed and 5 'Y' RCA Post incident learning and knowledgebase
	• AI/ ML powered Predictive analytics • Actionable Threat Intelligence	Cyber Fraud Intelligence Platform	Empanel and onboard First level responders, forensic partners	Regulatory framework as Capability driver
	• Zero Trust Architecture • Microsegmentation	Identity First and Credential Resilience	• Resilience testing • Red Team assessments	AI and PQC strategy
	Continuous Attack Surface visibility and Threat Exposure Management	Cloud Native and API security	Table Top exercises and Attack Simulation and response	Attract and retain Talent Right Sourcing
	Post Quantum Crypto readiness	Regulations around data protection and operational resilience	Cyber Insurance	Vulnerability prioritization and management

Implementing Cybersecurity Framework (NIST)

Governance	Identify	Protect	Detect	Respond & Recover
Board Oversight	Risk Assessments	Segmented networks	Advanced Cyber Defense Center	24/7 incident response teams, systems and processes
Security Policy	Asset management	Advanced edge controls	Threat intelligence services	First responder services
Roles and Responsibilities	Vulnerability assessments & penetration testing	Web application firewalls	Deception technologies	Security orchestration and remediation
Regulatory Compliance	Application security	DNS security systems	Network anomaly detection systems	Cyber Security crisis response plans
Automation	Data discovery	IDS & IPS systems	DDoS detection & mitigation systems	Cyber attack simulation
	Red Team assessment	Data protection & encryption	End point detection systems	Digital forensics
	Compromise Assessment	Multifactor authentication	Anti-phishing services	IR playbooks
	Attack surface management	Restricted access control	Social media monitoring	
	Application Threat modeling	Secure email controls systems	Brand reputation services	
		Hardened systems	Threat hunting	
		Virtual Patching	UEBA	
		Awareness	Cyber Analytics	



The Asymmetric Battlefield

Economic Asymmetry (Cost to Kill)

1. **The Attacker's Budget:** "R&D" is crowd-sourced. Use stolen infra to attack yours. Light, agile, $50 tools, *"Needs to be right once.*
2. **CISO's Budget:** 50+ security tools, $5M budget, *"Needs to be right 100% of the time*
3. **The ROI Gap**: An attacker's ROI is calculated in Bitcoin; a CISO's ROI is "nothing happened today" (which is hard to sell to a CFO).

For every $1 an attacker spends on a polymorphic script, a CISO spends $1,000 on licensing, integration, training, and monitoring.

Temporal Asymmetry (Clock)

1. **"Dwell Time" :** Attackers move in silence and wait for the "perfect storm" (e.g., a holiday weekend or a merger).
2. **The Defender's Race:** The CISO is always reactive to the "Alert."
3. **Data Point: A**verage time to identify and contain a cross environment breach is 276 days – IBM Cost of a Data Breach Report 2025

Cognitive Asymmetry (Human Factor)

1. **The "Script" vs. the "Social":** We spend millions on AI-driven firewalls, but the attacker wins with a $0 phone call pretending to be "Jim from IT."
2. **The AI Force Multiplier:** Generative AI has removed the "tells" of phishing (bad grammar, weird formatting). Now, the asymmetry is perfect: a low-skill attacker can generate high-skill deception.

The math is broken. We don't need a bigger shield; we need a different game."

Thought Insights

*Move from being **'The Wall'** to being **'The Immune System'."***

Asymmetric Winning: Flip the script

1. **Deception :** Plant "Honey-tokens" and fake data. Make the attacker spend *their* time and money chasing ghosts.
2. **Zero Trust 2.0 :** Don't try to keep them out of the "house"; authenticate every single door.
3. **Automation:** If an attacker uses a bot to scan you 10,000 times a second, use an AI that shuts down the port in a millisecond without a human in the loop.

THANK YOU

Any Questions ?

ICAI DX CONFERENCE

ISAS: The Future of Technology Audit and Assurance

Information Systems Audit Standards for Chartered Accountants

Anand Prakash Jangid
Chief Change Agent
Ajalabs.ai

Narasimhan Elangovan
Co-Founder and Cyber Security Practice Leader
Incorp Advisory Services

Session Overview

01 The New Audit Reality

Technology risk landscape and common myths

02 Why ISAS Matters

Framework, principles and purpose

03 Regulatory Landscape

RBI, SEBI, IRDAI, CERT-In and DPDP

04 ISAS Standards in Practice

Deep dive into each ISAS standard

05 Building Your ISAS Practice

Career, monetisation and getting started

06 Closing

Final message and the future of the profession

01

The New Audit Reality

Technology risk is business risk. Understanding the landscape that makes ISAS essential.

Emerging Technology Risks: The New Audit Reality

THE LANDSCAPE

- Core systems, cloud, APIs, AI, data lakes, fintech platforms and SaaS tools now run critical business processes.
- Errors in configuration, access rights, algorithms, interfaces or data flows can directly affect financial reporting, compliance and customer outcomes.

THE RISK CONVERGENCE

- Technology risk is now **business risk**.
- Technology risk is now **audit risk**.
- Technology risk is now **governance risk**.
- Technology risk is now **regulatory risk**.

THE ISAS RESPONSE

ISAS recognises that assurance over information systems, risk management and controls is **fundamental to governance and stakeholder confidence**.

The Mythos: Myths We Must Challenge

Common myths in boardrooms and audit rooms

- ✗ *"If it is automated, it must be accurate."*
- ✗ *"Cloud means the vendor owns the risk."*
- ✗ *"Cybersecurity is only the CISO's responsibility."*
- ✗ *"DPDP is only a legal compliance issue."*
- ✗ *"AI output is reliable because the model is advanced."*
- ✗ *"A SOC report is enough evidence."*
- ✗ *"IT audit is only for large banks."*
- ✗ *"VAPT is the same as cybersecurity audit."*

✓ **Reality:** CAs must challenge these assumptions through risk-based IS assurance.

Risks Across Sectors, Not Just Banking

Where IS audit risk is emerging — ISAS applies across all sectors

Banking / NBFCs

Core banking, digital lending, UPI, outsourcing, cyber resilience

Capital Markets

Algo trading, brokers, AMCs, KRAs, RTAs, exchanges

Insurance

Policy admin systems, claims platforms, intermediaries, customer data

Healthcare

Health data platforms, consent management, ABDM integrations

Manufacturing

ERP, OT, IoT, supply-chain systems

E-com / Fintech

Payment systems, APIs, customer data, fraud analytics

Govt / PSU

Citizen data, portals, cloud hosting, safe-to-host audits

ISAS applies wherever technology supports material business, compliance or governance processes.

What Was Missing Before ISAS?

Practical gaps the profession faced

THE GAPS

- No common Sovereign minimum benchmark for IS audit
- Inconsistent IS audit planning and documentation
- Confusion between assurance, advisory, VAPT and checklist reviews
- Weak linkage between business risk and technology risk
- Over-dependence on screenshots, management representations and vendor reports
- Limited quality-control and peer-review orientation for IS audit work

THE ISAS SOLUTION

ISAS addresses these gaps through a **principle-based framework** covering:

- Planning — structured engagement methodology
- Execution — approved work programs and procedures
- Evidence — sufficient, appropriate and reliable
- Reporting — clear, risk-rated and actionable
- Quality — continual improvement and peer review

02

Why ISAS Matters

A structured framework for professional technology assurance.

Why ISAS? Four Core Questions

ISAS helps CAs answer the fundamental questions of any assurance engagement

1 What is the subject matter?

ITGC, cybersecurity, DPDP, cloud, application controls or vendor risk?

2 What criteria are being used?

ISAS, RBI, SEBI, CERT-In, ISO, DPDP, or internal policy?

3 What assurance is being provided?

Reasonable assurance, limited assurance, attestation, AUP or advisory?

4 What evidence supports the conclusion?

Sufficient, appropriate, reliable and reproducible evidence?

ISAS 110 specifically deals with nature of assurance, IS governance, IS risk management, IS controls, and laws and regulations — giving CAs a structured starting point for every engagement.

Purpose of ISAS

ISAS is designed to achieve five key objectives

1 MINIMUM STANDARDS

Provide minimum standards for Information Systems Audit engagements

2 CLARITY FOR USERS

Give users clarity on the quality expected from IS audit services

3 REGULATOR CONFIDENCE

Help regulators understand the scope, depth and reliability of IS audit outcomes

4 PRACTICAL GUIDANCE

Guide professionals on practical implementation issues

5 PROFESSIONAL RIGOUR

Support consistency, discipline and professional rigour in IS audit engagements

ISAS Framework at a Glance

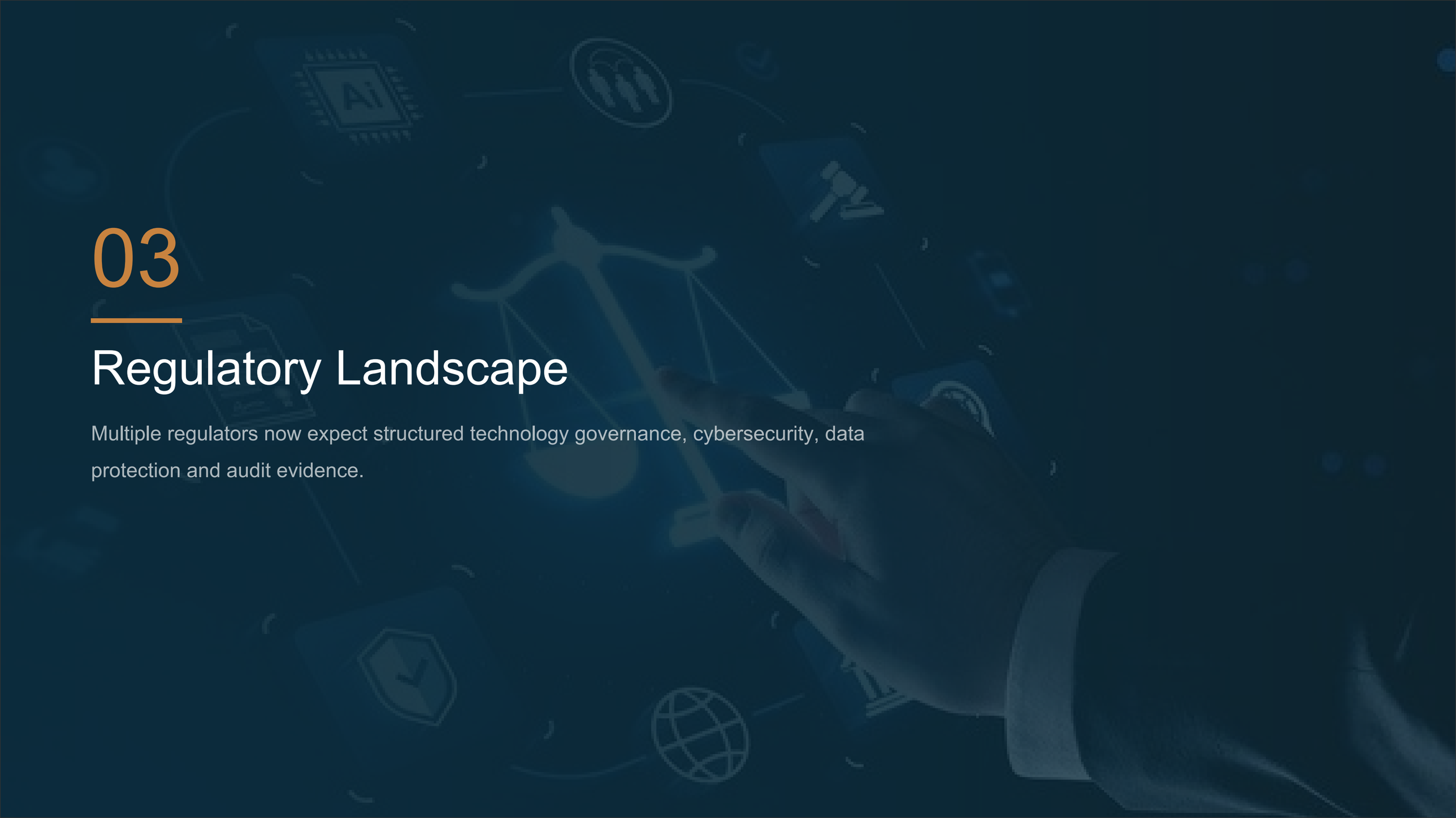
Component	Standard	Focus Area
Framework	Governing Information Systems Audit	Overarching governance and scope
Principles	Basic Principles	Professional ethics and conduct
ISAS 110	Key Concepts	Assurance types, subject matter, criteria
ISAS 210	Business and IS Context	Understanding the auditee's technology landscape
ISAS 220	Engagement Planning	Planning, experts, communication protocols
ISAS 310	Assignment Execution	Work programs, procedures, supervision
ISAS 320	Evidence and Documentation	Sufficient, appropriate, reliable evidence
ISAS 410	Audit of IS Controls	ITGC and application controls
ISAS 420	Automated Tools and Techniques	Analytics, AI, blockchain, big data
ISAS 430	Digital Personal Data Protection	DPDP lifecycle, privacy controls
ISAS 440	Cybersecurity Audit	Governance, protection, detection, response
ISAS 510	Reporting Results	Findings, risk ratings, recommendations
ISAS 610	Quality Management	Continual improvement, CPE, quality reviews

Basic Principles for CAs

ISAS is built on nine professional principles

- **Independence**
- **Integrity and Objectivity**
- **Due Professional Care**
- **Confidentiality**
- **Skills and Competence**
- **Aligned Business-IT Context**
- **Systematic Engagement Performance**
- **Effective Communication**
- **Quality and Continuous Improvement**

IS audit is not a casual IT checklist. It is professional assurance.



03

Regulatory Landscape

Multiple regulators now expect structured technology governance, cybersecurity, data protection and audit evidence.

Regulatory Expectations Are Converging

Key regulators and their technology governance expectations

RBI

IT governance, IT risk, controls, cyber resilience, IS audit and third-party arrangements

SEBI

CSCRF for SEBI-regulated entities, cyber resilience and cyber audit expectations

IRDAI

Information and Cyber Security Guidelines for insurers and intermediaries

CERT-IN

Comprehensive Cyber Security Audit Policy Guidelines covering audit planning, execution, evidence, reporting and quality control

DPDP

Privacy, breach response, data protection obligations and Significant Data Fiduciary compliance expectations. The Digital Personal Data Protection Act creates a new compliance frontier for organisations and auditors alike.

Regulatory Opportunity Map for CAs

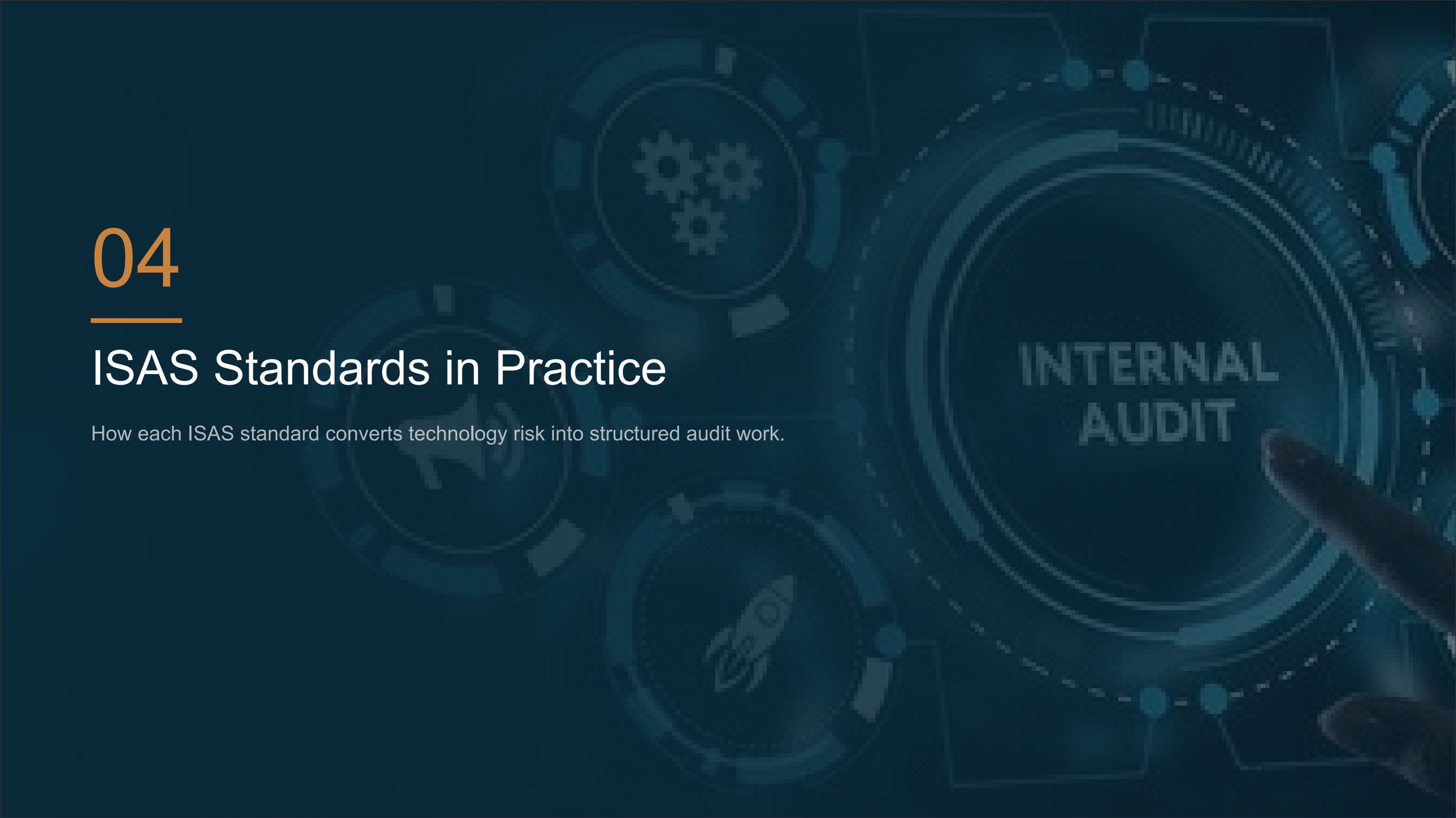
High-potential areas for ISAS-aligned assurance services

	Opportunity Area	Description
1	RBI IT governance and IS audit reviews	Technology risk assessment for banks and NBFCs
2	RBI outsourcing and third-party technology risk	Vendor due diligence and contract review
3	SEBI CSCRF compliance and cyber audit	Cyber resilience framework for capital markets
4	IRDAI information and cybersecurity assurance	Insurer and intermediary security reviews
5	DPDP readiness and privacy control reviews	Data protection gap assessment and remediation
6	CERT-In-aligned cybersecurity audit support	Formal cyber audit under CERT-In guidelines
7	Cloud governance and SOC report review	Vendor assurance and shared responsibility
8	AI / automated decisioning governance	Model governance and algorithm assurance
9	Internal audit co-sourcing for technology risk	Technology risk coverage for internal audit functions

04

ISAS Standards in Practice

How each ISAS standard converts technology risk into structured audit work.



How ISAS Converts Technology Risk into Audit Work

BEFORE ISAS

"Is IT okay?"

Generic, unstructured, no defined criteria, no assurance level, weak evidence.

WITH ISAS

"What is the business process, what systems support it, what risks arise, what controls exist, what evidence supports the conclusion?"

Structured, criteria-driven, risk-based, evidence-backed professional assurance.

The ISAS Framework defines **Information Systems Audit** as *independent assurance on the adequacy and effectiveness of information systems, controls and processes to manage risks aligned with enterprise business and governance objectives.*

ISAS 110

Key Concepts

WHAT THE STANDARD SAYS

ISAS 110 requires the Professional to understand:

- Nature of assurance
- IS governance and IS risk management
- IS controls and laws and regulations
- Subject matter and suitable criteria
- Information systems assertions
- Type of engagement

PRACTICAL RELEVANCE

Before accepting an IS audit, the CA must clarify:

- Is this **assurance, attestation, AUP or advisory**?
- What is the **subject matter**?
- What **criteria** will be used?
- What **opinion or conclusion** can be given?

EXAMPLE

A VAPT is usually closer to an **agreed-upon procedure**, while an ITGC review may be structured as an **assurance engagement**. ISAS 110 helps avoid mixing these up.

ISAS 210

Business and IS Context

WHAT THE STANDARD SAYS

ISAS 210 requires understanding the:

- Business, strategic, regulatory, operational landscape
- IS Universe and level of automation
- Applications, infrastructure, interfaces
- Third-party services
- Business-technology alignment

PRACTICAL RELEVANCE

The CA should first map:

- Key **business processes**
- **Applications** supporting those processes
- Critical **data flows** and interfaces
- **Third-party** dependencies
- Regulatory obligations and automation level

EXAMPLE

For an NBFC digital lending process, map the loan origination system, credit bureau API, underwriting engine, bank account verification, disbursement interface, collection system and regulatory reporting **before** designing audit procedures.

ISAS 220 Engagement Planning

WHAT THE STANDARD SAYS

ISAS 220 requires a process-driven engagement plan covering:

- Mandate, objectives and scope
- Business and IS understanding
- Risk environment and stakeholders
- Resource competence and expert involvement
- Communication protocols

PRACTICAL RELEVANCE

Useful when planning:

- Annual IS audit plan and cyber audit
- DPDP readiness and cloud review
- ERP controls review and vendor risk assessment
- Regulatory compliance review

EXAMPLE

If a CA firm performs a cybersecurity governance review, it may engage a technical expert for vulnerability validation. ISAS 220 requires the CA to **evaluate and supervise the expert** — not blindly attach the expert's report.

ISAS 310

Assignment Execution

WHAT THE STANDARD SAYS

ISAS 310 requires:

- Assignment-level planning
- Approved audit work programs
- Defined procedures and adequate resources
- Review and supervision
- Sufficient evidence and professional scepticism
- Risk-based evaluation of findings

PRACTICAL RELEVANCE

Every IS audit assignment should have:

- Assignment objective and scope boundary
- Criteria and risk assessment
- Work program and evidence requirements
- Responsibility allocation
- Review trail and risk-rated findings

EXAMPLE

For user access review, the work program should not simply say "obtain user list." It should specify systems covered, privileged users, joiner-mover-leaver testing, maker-checker conflicts, dormant users, admin IDs, and evidence to be retained.

ISAS 320

Evidence and Documentation

WHAT THE STANDARD SAYS

ISAS 320 requires **sufficient, appropriate and reliable** IS audit evidence including:

- Direct and supporting evidence
- Context-specific evidence
- Digital artifacts — logs, configs, metadata
- Network traffic data and screen recordings
- Traceability, repeatability, integrity
- Secure storage and chain of custody

PRACTICAL RELEVANCE

CAs must ask:

- Is the evidence **system-generated** or manual?
- Is it **complete** and independently reperformable?
- Are **timestamps, logs or audit trails** available?
- Has evidence been **securely obtained and retained**?
- Is **chain of custody** relevant?

EXAMPLE

For a cyber incident review, screenshots of logs are weak evidence. Better: exported logs, ticket history, SIEM alerts, backup restoration records, incident timeline, hash values and management action records.

ISAS 410 Audit of IS Controls

WHAT THE STANDARD SAYS

ISAS 410 covers audit of IS controls including:

- IT general controls (ITGC)
- Application controls
- Entity-level and technical controls
- Service provider controls
- Automated and IT-dependent manual controls

PRACTICAL RELEVANCE

Typical audit areas:

- User access and privileged access
- Change management
- Backup, restoration, job monitoring
- Incident management and audit trails
- Application configuration and maker-checker
- Automated calculations and interface controls

EXAMPLE

In an ERP audit, ISAS 410 helps test whether invoice approval workflows, user roles, segregation of duties, master data changes and automated tax calculations are **properly designed and operating effectively**.

ISAS 420 Automated Tools and Techniques

WHAT THE STANDARD SAYS

ISAS 420 covers use of automated tools:

- Analytics, AI, blockchain, big data
- Tool selection and competence
- Governance, validation, risk assessment
- Data integrity and confidentiality
- Professional scepticism and reproducibility

PRACTICAL RELEVANCE

Applies in two ways:

- When the **auditor uses tools** for audit procedures
- When the **auditee uses AI/automation** in business

Key questions: Is the tool validated? Is data complete? Can output be reproduced? Is there bias? Are exceptions reviewed?

EXAMPLE

For AI-based credit scoring or fraud analytics, the CA can examine data inputs, model governance, approval process, exception handling, monitoring and **reproducibility of results**.

ISAS 430 Digital Personal Data Protection

WHAT THE STANDARD SAYS

ISAS 430 covers audit of DPDP:

- Digital personal data lifecycle
- Privacy controls and outsourcing
- Vendor assurance and data sharing
- Technical measures — profiling, cookies
- Pseudonymisation and anonymisation
- Compliance with data protection laws

PRACTICAL RELEVANCE

Audit focus areas for DPDP readiness:

- Personal data inventory and consent mapping
- Data collection notices and vendor sharing
- Access controls and retention/deletion
- Breach response and masking in test environments
- Data processor contracts and cross-border transfers

EXAMPLE

For a healthcare platform, the CA can review whether patient data is mapped, access is restricted, consent is captured, vendors are contractually bound and **breach-response procedures exist**.

ISAS 440 Cybersecurity Audit

WHAT THE STANDARD SAYS

ISAS 440 requires risk-aligned cybersecurity audit:

- Governance and asset inventory
- Layered controls — protection, detection, response, recovery
- Third-party cyber risk
- Documentation of activities, controls, findings

PRACTICAL RELEVANCE

Cybersecurity audit covers more than firewall and antivirus:

- Cyber governance and asset inventory
- Vulnerability management and MFA
- Endpoint protection and log monitoring
- Incident response and backup/recovery
- Cyber drills and third-party cyber risk

EXAMPLE

For a ransomware readiness review, the CA checks whether backups are protected, restoration is tested, incident response roles are defined, privileged access is controlled and **cyber incidents are escalated to management**.

ISAS 510

Reporting Results

WHAT THE STANDARD SAYS

ISAS 510 provides reporting structure:

- Identification, scope, management responsibility
- Executive summary and findings
- Risk rating and key IS audit matters
- Agreed-upon procedures
- Actionable recommendations

PRACTICAL RELEVANCE

Avoid vague reporting. Every finding should include:

- **Condition, criteria, cause**
- **Risk/impact** and evidence
- **Management response**
- **Recommendation** with timeline
- **Residual risk** and responsibility

EXAMPLE

Instead of "vendor monitoring is weak," report: critical service providers are not risk-rated, SOC reports are not reviewed, right-to-audit clauses are absent — creating **operational, regulatory and data protection risk**.

ISAS 610 Quality Management

WHAT THE STANDARD SAYS

ISAS 610 focuses on quality:

- Structured quality processes
- Appropriate staffing and competence
- Quality reviews and monitoring
- CPE requirements
- Documentation of the QMS

PRACTICAL RELEVANCE

For firms scaling IS audit work:

- Create IS audit methodology
- Maintain standard workpaper templates
- Conduct engagement quality review
- Train team and maintain competence records
- Review expert work and track improvements

EXAMPLE

A CA firm offering DPDP and cyber reviews should not operate with ad hoc checklists. It should maintain templates, review notes, evidence standards, **expert evaluation records and quality review documentation**.

Practical Relevance Across Opportunities

Opportunity	Relevant ISAS	Practical Output
ITGC review	ISAS 210, 310, 320, 410	Controls design and operating effectiveness report
Cybersecurity review	ISAS 220, 320, 440, 510	Cyber risk and governance assurance report
DPDP readiness	ISAS 110, 210, 320, 430	Privacy gap assessment and remediation roadmap
Cloud / vendor risk	ISAS 210, 220, 320, 410, 440	Third-party technology risk report
AI / analytics review	ISAS 420, 320, 430	Model governance and data-risk review
Audit committee reporting	ISAS 510	Risk-rated technology assurance report
IS audit practice building	ISAS 610	Quality-controlled IS audit methodology

06

Building Your ISAS Practice

Career pathways, monetisation strategies and practical steps to get started.

How Can a CA Monetise ISAS?

Convert ISAS into structured service offerings

- ISAS-based ITGC review
- Cyber governance review
- DPDP readiness assessment
- Vendor / cloud risk review
- Internal audit technology-risk co-sourcing
- SEBI CSCRF readiness support
- RBI IT governance gap assessment
- Audit committee technology-risk reporting

"Not IT consulting alone — professional assurance using ICAI's ISAS framework."

Creating the Conversation + Getting Started

CREATE THE CONVERSATION

A CA should not wait for a client to ask for "ISAS audit." They should create the conversation.

- Start with existing audit or advisory clients
- Ask whether technology supports key financial or compliance processes
- Offer a small diagnostic review
- Begin with one area: access, change, vendor risk or DPDP
- Use ISAS language to show professional structure
- Partner with technical experts where needed

FOR SMALL FIRMS: 7 STEPS

1. Read ISAS Framework, Basic Principles and ISAS 110
2. Build one simple ISAS-aligned template
3. Pick one service line — ITGC, DPDP or vendor risk
4. Train one partner and two team members
5. Co-source technical areas like VAPT or cloud security
6. Pilot with an existing client
7. Convert the pilot into a repeatable offering

Do not start with everything. Start with one practical use case.

Industry CA or Practice CA — Who Benefits More?

CA IN INDUSTRY

Can use ISAS for:

- Internal audit planning
- Audit committee reporting
- Vendor governance
- Cyber and DPDP readiness
- Regulatory inspection preparedness
- Control self-assessment

CA IN PRACTICE

Can use ISAS for:

- New assurance services
- Co-sourcing with companies
- Regulatory readiness reviews
- Cyber governance reviews
- DPDP and vendor-risk engagements
- IS audit quality differentiation

Building a Career in IS Audit

Suggested career path for CAs entering technology assurance

1

Start with ITGC and application controls

2

Learn business process and system dependency mapping

3

Move into cybersecurity, cloud risk, DPDP, vendor assurance

4

Build one regulatory specialisation — RBI, SEBI, IRDAI, DPDP or CERT-In

5

Add one technical-adjacent skill — data analytics, cloud security, privacy or ISO 27001

6

Develop reporting skills for audit committees and boards

> The CA who understands both business risk and technology risk will be highly relevant.

What Should CAs Avoid?

Common pitfalls that undermine professional credibility

- ✕ Calling every IT review an "audit" without defined criteria
- ✕ Giving assurance without defining criteria
- ✕ Over-relying on screenshots as evidence
- ✕ Blindly relying on vendor or expert reports
- ✕ Treating cybersecurity as only VAPT
- ✕ Treating DPDP as only legal documentation
- ✕ Reporting generic observations without risk and action plan
- ✕ Accepting engagements without required competence

The Best First ISAS-Based Offering

For small / mid-sized firms — practical starting points

- **ITGC review**
- **DPDP readiness assessment**
- **Vendor risk review**
- **Cyber governance gap assessment**
- **SOC report review**
- **ERP access and change management review**

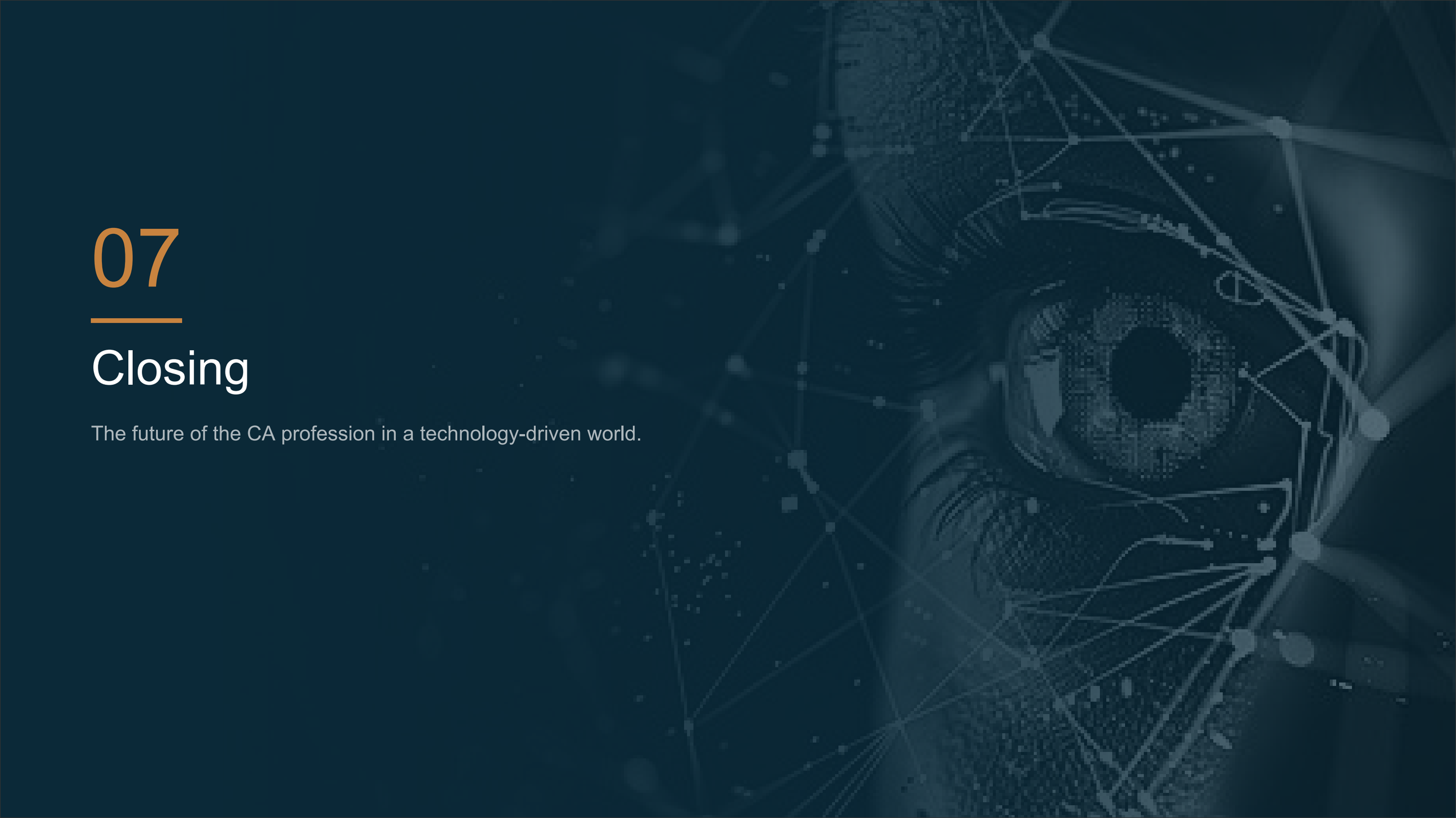
WHY THESE FIRST?

- They are **understandable to existing clients** — no need to explain complex technology concepts
- They **connect directly with internal controls** — building on what CAs already know
- They require **audit discipline more than deep coding skills**
- They can be **delivered with limited but trained teams**
- They **open the door to larger engagements** — cyber, privacy and regulatory work

07

Closing

The future of the CA profession in a technology-driven world.

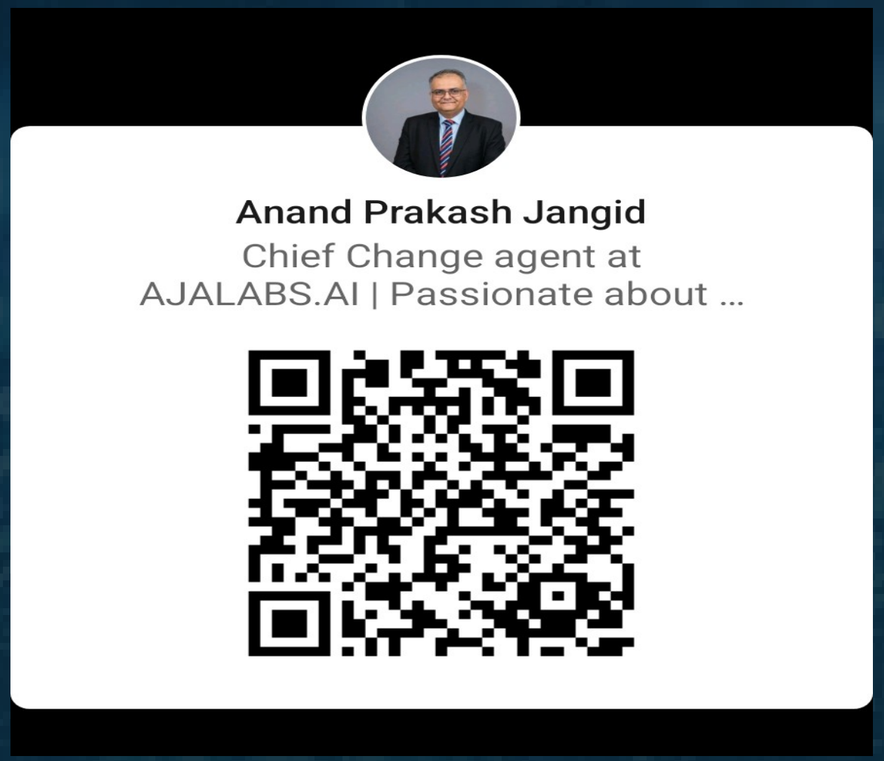


Final Message

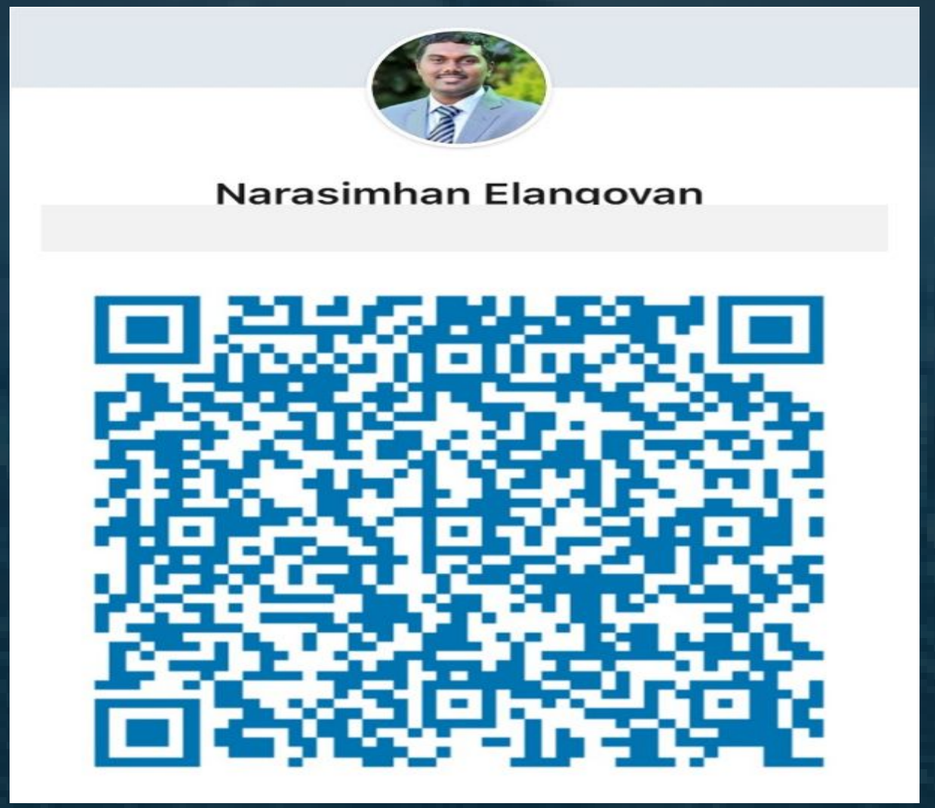
ISAS is not only about technology. It is about:

- **Trust**
- **Governance**
- **Evidence**
- **Assurance**
- **Regulatory confidence**
- **Professional relevance**

"The future CA will not only audit financial numbers. The future CA will also provide assurance on the systems, data, controls and technologies that create those numbers."



THANK YOU



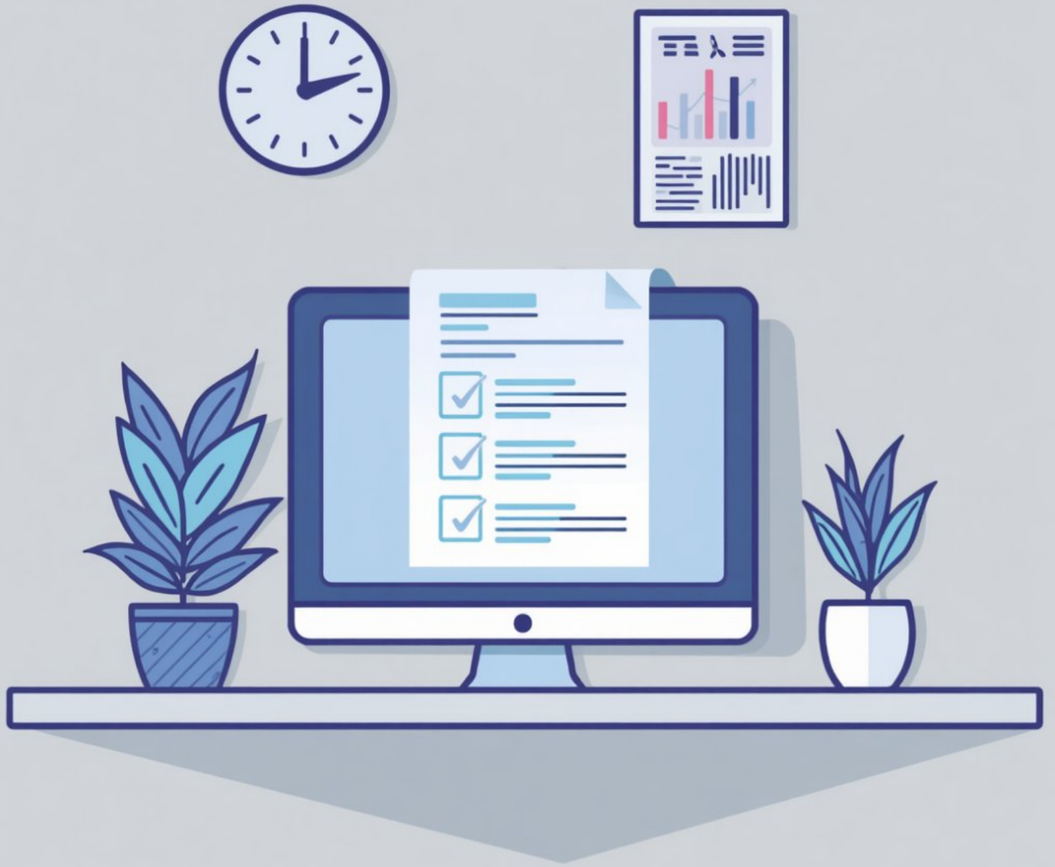
Anand Prakash Jangid
Chief Change Agent
Ajalabs.ai

Narasimhan Elangovan
Co-Founder and Cyber Security Practice Leader
Incorp Advisory Services

Evolving Data Driven Tax Administration and Enforcement

Taxpayer Compliance Simplified

Enhancing taxpayer experience through **AIS data**, pre-filled ITRs, and quick refunds fosters **confidence** and streamlines the overall compliance process in the digital age.



SFT Reporting: Detection of Evasion

HIGH-VALUE TRANSACTIONS

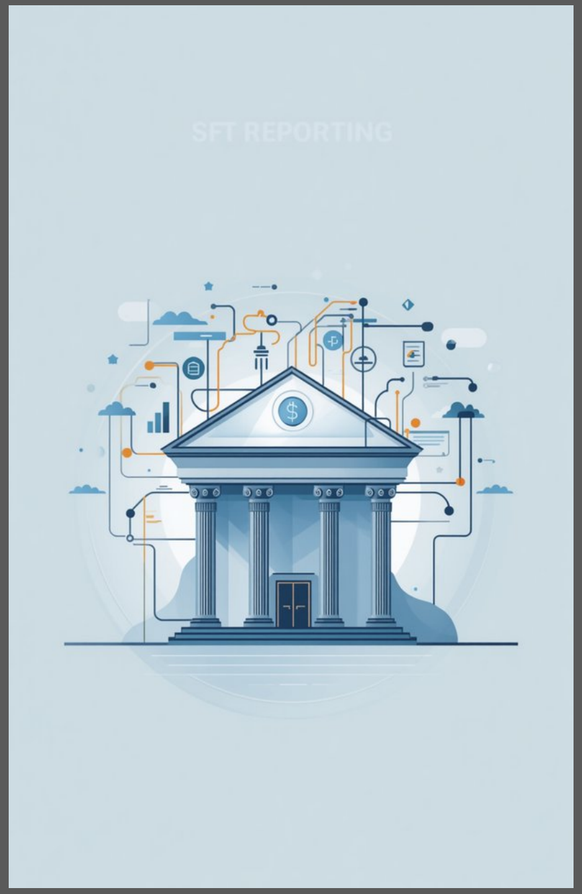
Data Insights

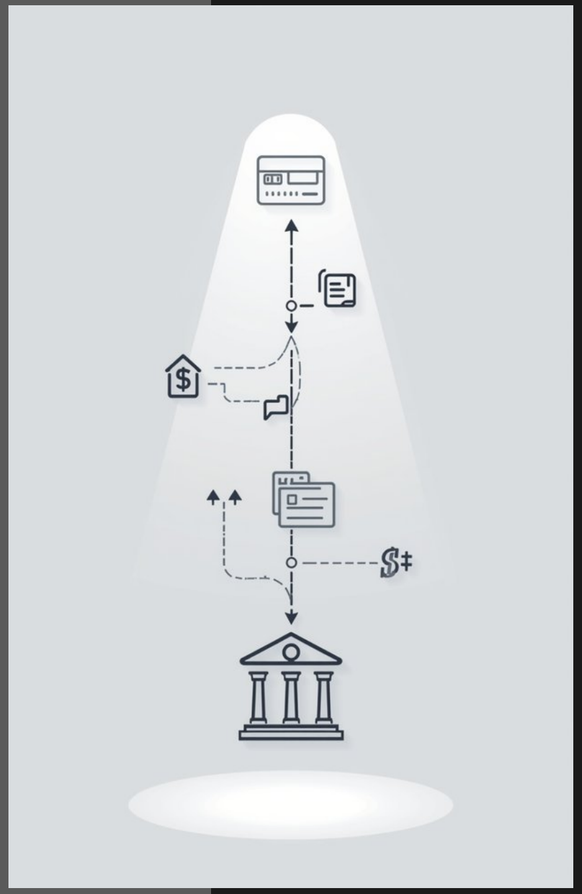
REPORTING ENTITIES

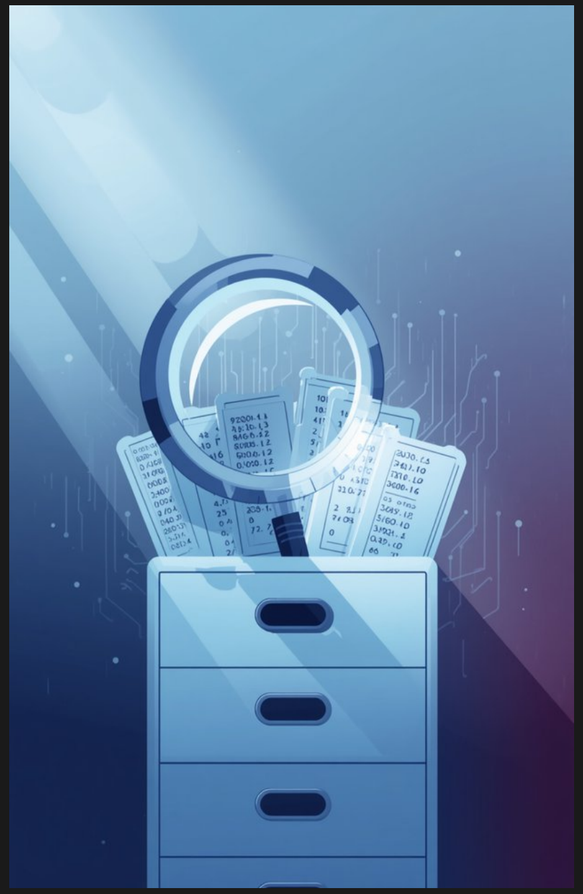
Financial Institutions

RISK IDENTIFICATION

Mismatch Cases







Digital Evidence in Taxation

CENTRAL ROLE

Digital evidence gathering is crucial for curbing tax evasion, enabling authorities to access various **electronic records** and data sources that facilitate comprehensive investigations.

LEGAL RECOGNITION

The Income-tax Act, 2025 acknowledges the validity of electronic records and computer systems, ensuring that digital material is admissible in legal proceedings against tax evaders.

VDA Taxation Overview

TAXATION PROVISIONS

Provisions under the new law address the taxation of income generated from the transfer of Virtual Digital Assets, ensuring clarity and compliance for taxpayers involved in such transactions.

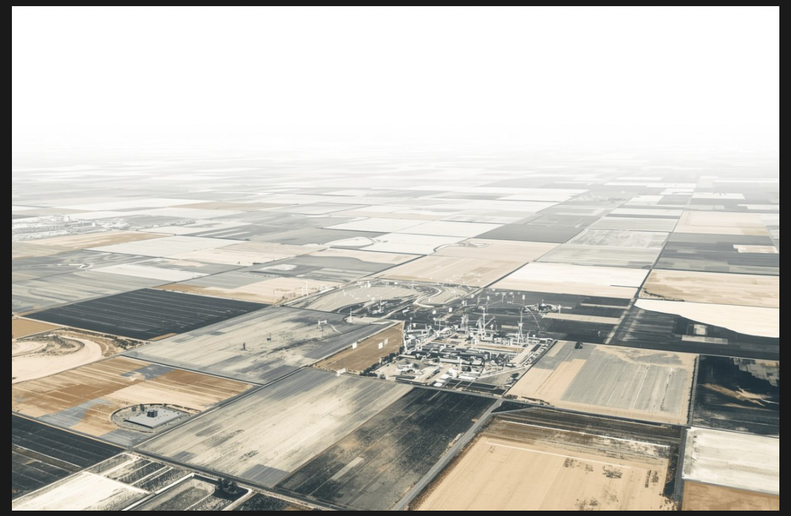
DEDUCTION RESTRICTIONS

The law imposes specific restrictions on deductions, set-off, and carry forward of losses related to Virtual Digital Assets, creating a structured framework for tax treatment and compliance.

REPORTING MECHANISMS

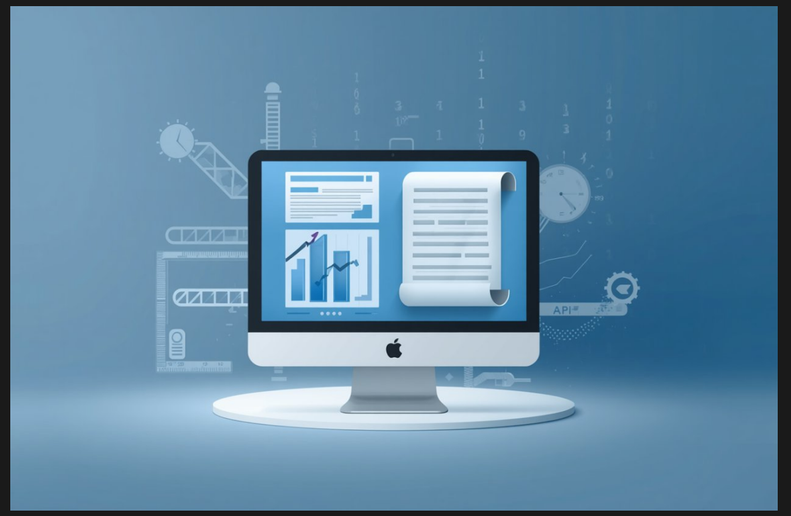
Enhanced reporting requirements and TDS mechanisms are introduced to establish transaction trails, facilitating investigations and ensuring accountability in Virtual Digital Asset transactions.

Technology in Investigation



SATELLITE DATA

Bogus claim of Agricultural Income through NRSC data.



AI DOCUMENT ANALYSIS

Bogus claim of cost of improvement by Font Analysis using AI.

DATA INVESTIGATION

A skilled team analyzes data to uncover fraud, strengthening evidence through technology-driven methods.

Large-Scale ESS Detection

ELECTRONIC SALES SUPPRESSION

Electronic Sales Suppression (ESS) involves the manipulation of billing systems, leading to deliberate deletion or modification of sales records to evade taxes.

DATA ANALYSIS TECHNIQUES

Comprehensive analysis of billing data reveals discrepancies such as deleted bills and abnormal cancellations, helping to identify ESS practices within businesses.

TRANSACTION COMPARISON

Comparing Point of Sale (POS) data with bank receipts and ITR filings uncovers systematic mismatches, ensuring accurate representation of turnover and tax liability.

LESSONS LEARNED

Structuring digital data facilitates the identification of ESS, allowing for proactive measures against systematic suppression and enhancing overall compliance efforts.

Leveraging Technology: A shift from Compliance by Deterrence to Compliance by Design

Technology plays a crucial role in transforming tax compliance. By integrating built-in compliance support, we can significantly reduce information asymmetry. This shift allows for more **targeted enforcement** and fosters a framework where compliance becomes easier, while evasion is increasingly difficult.

Thank You

DxFS 2026 · DAAB ICAI

From Data to Decisions

Practical AI for accounting, audit, forensics and the businesses you advise.

Rishabh Prakash

Engineer · Building AI tools for finance and security workflows

22 May 2026 · Novotel Hyderabad Convention Centre

30 MINUTES · WHAT WE'LL COVER

From layers, to live use cases, to Monday morning.

01

10 min

The Frame

Three layers of data, four AI model buckets, the audit-trail principle. Why it matters before any tool decision.

02

18 min

13 Live Use Cases

Six for the businesses you advise. One for your audit practice. Six for forensics, DPDP, and data security.

03

2 min

Three Monday Actions

What to try this week — for your firm, your clients, and every AI tool you evaluate.

PART 01

The Frame

Three layers. Four model tiers. One audit trail rule.

THE THESIS

Data → Decisions is three layers, not one.

01

Extraction

Messy in, clean out

PDF invoice → fields
Bank statement → table
Email → structured request

Cheap models. 90% of work.

02

Reasoning

Clean data → judgment

Is this transaction unusual?
Is this RPT material?
Does this clause apply?

Mid-tier models. 9% of work.

03

Decision

Judgment → action

Draft notice reply
Flagged audit sample
Approve or reject

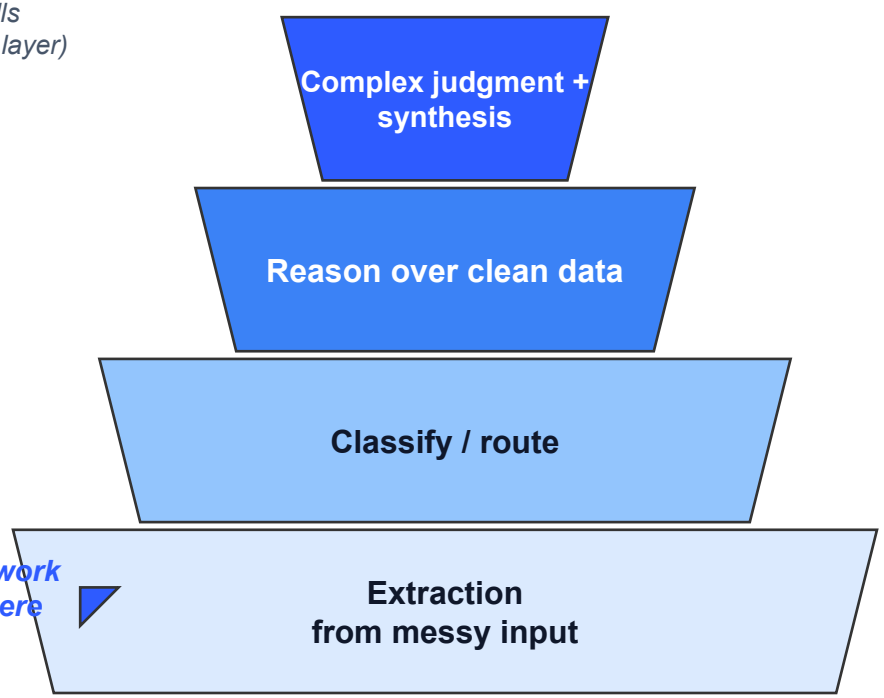
Premium models. 1% of work.
Your billable layer.

Your billing power has always lived at Layer 3. AI just cut the cost of Layers 1 and 2 by 50–100×.

MODEL SELECTION

Choose the right AI for the right job.

Premium tier
1% of calls
(your billable layer)



Complex judgment + synthesis
Claude Opus 4.7 · Gemini 3.1 Pro
₹2,500–₹6,000
/ 1,000 jobs

Reason over clean data
Claude Sonnet 4.6 · Gemini 2.5 Pro
₹400–₹1,200
/ 1,000 jobs

Classify / route
Gemini 2.5 Flash-Lite · Claude Haiku 4.5
₹10–₹25
/ 1,000 jobs

Extraction from messy input
Gemini 2.5 Flash-Lite · Claude Haiku 4.5
₹15–₹40
/ 1,000 jobs

90% of calls go to cheap models. 10% to expensive ones. If your AI bill looks the opposite, your architecture is wrong.

Sources: Anthropic API pricing (Jan 2026); Google AI pricing (May 2026). Costs assume ~1,500 input + ~500 output tokens per job; 1 USD ≈ ₹83.

WORKED EXAMPLE

Reconciling 5,000 invoices for under ₹20.

1

Parse GSTR-2B JSON + purchase register

₹0

Pure code

2

Match by GSTIN + amount + date

₹0

Pure code

3

Generate one-line 'why not matched'

₹15

Gemini Flash-Lite
× 5,000 calls

4

Partner-ready summary narrative

₹3

Sonnet 4.6
× 1 call

Total AI cost

≈ ₹18

To do what currently costs a junior 6 hours of manual matching.

Cost estimate: 5,000 vendor rows; avg 1,000 input + 200 output tokens per Flash-Lite call; 8,000 in + 1,500 out for the Sonnet summary. Prices per Anthropic and Google official pricing pages (Jan 2026, May 2026).

THE NON-NEGOTIABLE RULE

No audit trail. No AI.

If you can't click an AI output and see the source row, page, or document — the tool is not built for your profession.

This is the single filter for every AI vendor pitch you hear.

Source citations on every output

Each row, ratio, or recommendation links to the document, page number, ledger entry, or formula it came from.

Reasoning trail, not a black box

Why did the AI flag this? What rule fired? What pattern matched? Click and see — not 'because AI'.

Reproducible results

Same input, same output. If outputs change every run, the tool is unsafe for audit defence.

PART 02 / A

AI for the businesses you advise.

Six agentic workflows your SME clients can build now.

- A1 Multi-channel customer journey orchestrator
- A2 Predictive micro-cohort marketing engine
- A3 Sales call intelligence pipeline
- A4 Dynamic pricing engine for SMEs
- A5 Demand forecasting with Indian calendar overlay
- A8 Operations exception agent

One agent. Four channels. Zero memory gaps.

Multi-channel customer journey orchestrator for SME businesses.

Cost / interaction:
₹0.50 vs ₹500

Inbound across 4 channels → Unified profile lookup → Channel-aware reply drafting → Sentiment + LTV scoring → **Send / escalate to human**

01

3 wks

TIME TO BUILD

02

200

/ month
HOURS SAVED

03

₹4K

/ month
COST TO RUN

STACK

Haiku 4.5 for chat at volume · Sonnet 4.6 for sentiment & escalation reasoning · Embeddings for profile match.

Sources: Kodif AI Customer Support Statistics (Nov 2025); Gartner Customer Service Research (Mar 2025); Anthropic API pricing (Jan 2026).

Stop blast emails. Start cohort surgery.

Predictive micro-cohort marketing engine — first-party data, autonomously segmented.

27% drop in personalisation cost

Sales + CRM data ingest → Cohort auto-discovery → Creative gen per cohort → Multi-channel A/B run → **Lift report + next cycle**

01

5 wks

TIME TO BUILD

02

60

/ month

HOURS SAVED

03

₹5K

/ month

COST TO RUN

STACK

Flash-Lite for cohort tagging at scale · Sonnet 4.6 for per-cohort creative · Embedding model for clustering.

Sources: ChatSpark Cost Analysis 2025; ChatMaxima AI Statistics 2026; Google AI Developer pricing (May 2026).

Every lost deal, explained. Every winning rep, copied.

Sales call intelligence — every call transcribed, patterns surfaced, coaching automated.

92% AI intent accuracy

Call recording (any source) → Multilingual transcription → Objection / signal extract → Pattern mining across deals → **Coaching brief per rep**

01

4 wks

TIME TO BUILD

02

80

/ month

HOURS SAVED

03

₹8K

/ month

COST TO RUN

STACK

Whisper / Gemini Flash for transcription · Haiku 4.5 for objection extraction · Sonnet 4.6 for weekly coaching brief.

Sources: ChatMaxima AI Customer Support Statistics 2026 (citing Google Cloud intent benchmark); Anthropic + Google API pricing.

A4 · CLIENT BUSINESS · PRICING OPS

Re-price every hour. Explainable. Reversible.

Dynamic pricing for restaurants, retail and services — quiet micro-optimisation, not surge.

5–15% revenue uplift typical

Inventory + sales feed → Competitor price scrape → Demand pattern learning → Hourly price recommendation → **Owner-review + auto-publish**

01

7 wks

TIME TO BUILD

02

40

/ month

HOURS SAVED

03

₹2K

/ month

COST TO RUN

STACK

Statistical forecasting model (no LLM) · Flash-Lite for competitor scrape & categorisation · Sonnet 4.6 for the daily 'why this price' note.

Sources: McKinsey Dynamic Pricing Studies; NRAI India F&B Report 2024; Anthropic + Google AI pricing.

Forecasts that know Diwali, monsoon, and the IPL final.

Demand forecasting with full Indian calendar overlay — auto-drafts purchase orders.

15–25% inventory reduction typical

3 years sales data → Calendar + weather overlay → SKU-level forecast → PO draft generation → **Owner approves or edits**

01

7 wks

TIME TO BUILD

02

50

/ month

HOURS SAVED

03

₹3K

/ month

COST TO RUN

STACK

Time-series forecasting (Prophet, NeuralProphet — no LLM cost) · Sonnet 4.6 for narrative report and exception explanations.

Sources: McKinsey Supply Chain & Operations Practice (2024); NRAI India F&B Report 2024; Anthropic API pricing.

Four dashboards no one opens. Replaced by alerts that matter.

Operations exception agent — watches ERP, CRM, POS in real time and routes anomalies.

45% fewer escalations

Real-time ERP / CRM feed → Anomaly detection → Context assembly → Right-person routing → **Action + log closure**

01

5 wks

TIME TO BUILD

02

120

/ month

HOURS SAVED

03

₹5K

/ month

COST TO RUN

STACK

Statistical anomaly detection (no LLM cost) · Flash-Lite for context summarisation · Sonnet 4.6 for high-value anomaly reasoning.

Sources: ChatMaxima AI Statistics 2026 (Gartner data on AI-agent escalation rates); Anthropic + Google API pricing.

PART 02 / B

Inside your audit practice.

The audit workflow AI can transform today.

- **B2** Cross-period audit anomaly detection (5-year drift)

Five years of drift. Found in five minutes.

Cross-period audit anomaly detection — partner brief with hypotheses before fieldwork starts.

₹36,014 cr
bank fraud FY25

5-year TB + ledger ingest → Ratio + ratio-of-ratio calc → Pattern drift detection → Hypothesis generation → **Partner brief + audit plan**

01

9 wks

TIME TO BUILD

02

60

/ audit

HOURS SAVED

03

₹1K

/ audit

COST TO RUN

STACK

Pandas / statistical analysis for ratio drift · Sonnet 4.6 for hypothesis generation · Opus 4.7 for final partner brief synthesis.

Sources: RBI Annual Report 2024-25 (May 2025); RBI Report on Trend and Progress of Banking 2024-25 (Dec 2025); Anthropic API pricing.

PART 02 / C

Forensics, DPDP, data security.

Six engagements where CAs become indispensable in the digital trust economy.

- C1 Data classification + access control perimeter for CA firms
- C2 Forensic email + chat reconstruction for fraud investigation
- C3 Shell company network mapping (MCA + bank + GST)
- C5 Synthetic data generator for safe vendor sharing
- C8 Zero-knowledge encrypted vault for client files
- C10 Cross-border data residency mapper

C1 · DPDP + ACCESS CONTROL · FOR YOUR FIRM

DPDP is here. Your file cabinet isn't ready.

Data classification + access control perimeter for your CA firm — DPDP-defensible by design.

₹250 cr max
DPDP penalty

Document ingestion → Sensitivity auto-tagging → Role-based access control → Access logging + audit trail → **Quarterly compliance report**

01

7 wks

TIME TO BUILD

02

60

/ month
HOURS SAVED

03

₹5K

/ month
COST TO RUN

STACK

Haiku 4.5 for document classification at ingestion · Sonnet 4.6 for quarterly compliance narrative · Pure code for logging and access control.

Sources: DPDP Act 2023, Schedule to Section 33; IBM Cost of a Data Breach Report India 2025 (Aug 2025); ICAI Student and Member Report 2025.

C2 · FORENSIC · FRAUD INVESTIGATION

Years of deleted threads. Reconstructed in hours.

Forensic email + chat reconstruction — court-admissible evidence chain from PST, Slack, WhatsApp dumps.

22.68 lakh cyber incidents in 2024

PST + chat dump ingest → Entity / actor resolution → Timeline reconstruction → Anomaly + gap detection → **Evidence chain report**

01

10 wks

TIME TO BUILD

02

300

/ case

HOURS SAVED

03

₹15K

/ case

COST TO RUN

STACK

Haiku 4.5 for thread-level extraction · Sonnet 4.6 for entity resolution and timeline · Opus 4.7 for the final court submission narrative.

Sources: PIB Press Release on Cyber Frauds (Oct 2025); RBI Annual Report 2024-25; APCERT Annual Report 2024; Anthropic API pricing.

C3 · FORENSIC · AML + SHELL COMPANY DETECTION

Follow the money. As a graph.

Shell company network mapping — MCA + bank + GSTIN triangulation into a single investigative diagram.

40,949 companies struck off in 3 yrs

MCA + GSTIN + bank ingest → Director graph construction → Pattern detection → Network visualisation → **Investigative report**

01

12 wks

TIME TO BUILD

02

200

/ case

HOURS SAVED

03

₹8K

/ case

COST TO RUN

STACK

Graph database (Neo4j-style) for entity relationships · Sonnet 4.6 for cluster hypothesis · Opus 4.7 for the investigative narrative.

Sources: Lok Sabha Unstarred Question Reply (21 July 2025), Ministry of Corporate Affairs; IndiaCSR (Nov 2024); Anthropic API pricing.

C5 · DPDP · DATA SHARING

Share everything. Expose nothing.

Synthetic data generator — statistical fidelity preserved, PII eliminated, DPDP-clean by design.

17% breaches via third-party

Real dataset profiling → Statistical fingerprint → Synthetic data gen → Privacy + utility validation → **Vendor handover (DPDP-clean)**

01

5 wks

TIME TO BUILD

02

50

/ dataset

HOURS SAVED

03

₹1K

/ dataset

COST TO RUN

STACK

Open-source synthetic libraries (SDV, ydata-synthetic — no LLM) · Sonnet 4.6 for privacy & utility validation report.

Sources: DPDP Act 2023, Schedule (Section 33); IBM Cost of a Data Breach Report India 2025; DPDP Rules 2025.

C8 · DATA SECURITY · FOR YOUR FIRM

Client files, defensible by design.

Zero-knowledge encrypted vault — time-bound links, watermarked downloads, tamper-evident logs.

₹22 cr avg India breach cost 2025

Encrypted upload → Zero-knowledge link generation → Watermarked download → Tamper-evident log → **Auto-expiry + revocation**

01

5 wks

TIME TO BUILD

02

40

/ month

HOURS SAVED

03

₹3K

/ month

COST TO RUN

STACK

Cryptography: AES-256 + envelope encryption (no LLM) · Haiku 4.5 for anomalous-access detection on the audit log.

Sources: IBM Cost of a Data Breach Report India 2025 (Aug 2025) — India highest globally; DPDP Act 2023; ICAI Guidelines on E-Filing.

C10 · DPDP + GLOBAL COMPLIANCE

Where your client's data lives. And what could fine them for it.

Cross-border data residency mapper — DPDP, GDPR, sector regulators in one compliance view.

DPDP enforcement: May 2027

Data system inventory → Data flow mapping → Jurisdiction risk overlay → Gap analysis → **Remediation roadmap**

01

9 wks

TIME TO BUILD

02

200

/ client

HOURS SAVED

03

₹10K

/ client

COST TO RUN

STACK

Code-based system discovery · Sonnet 4.6 for jurisdiction risk reasoning · Opus 4.7 for the final remediation roadmap.

Sources: DPDP Act 2023 (Section 8(6), Schedule); DPDP Rules 2025; Rainmaker Legal '18-Month DPBI Action Plan' (Jan 2026).

WHAT TO DO NEXT

Three actions for Monday morning.

01

For your firm

Pick the one workflow eating the most junior billable hours. If it's deterministic, that's automation target #1. Allocate one engineering week to prototype it.

02

For your clients

Pick one of the six client-business use cases that matches your largest client. Pitch it this week — even before you know how to build it. The conversation itself repositions you as a digital advisor, not a compliance vendor.

03

For every AI tool you evaluate

Demand audit trail. No source-row trace = no purchase. This single filter eliminates 80% of pitches that will land in your inbox over the next 12 months.

EVERY NUMBER, CITED

Sources.

1. DPDP Act 2023, Schedule to Section 33 (penalties); DPDP Rules 2025. (dpdpa.com, Rainmaker Legal, Jan 2026)
2. Reserve Bank of India, Annual Report 2024-25, Chapter on Frauds (May 2025). Fraud value ₹36,014 cr in FY25.
3. IBM, Cost of a Data Breach Report — India 2025 (Aug 2025). ₹220 million avg breach cost; 263-day lifecycle.
4. Ministry of Corporate Affairs, Lok Sabha Unstarred Question Reply (21 July 2025). 40,949 companies struck off in 3 years.
5. PIB Press Release, 'Curbing Cyber Frauds in Digital India' (Oct 2025). 22.68 lakh cyber incidents in 2024 per CERT-In.
6. Ministry of MSME, PIB Press Release (Feb 2026). 7.83 crore MSMEs registered on Udyam Registration Portal.
7. ICAI, Student and Member Report 2025. 4,07,629 members; 98,967 registered firms.
8. FBI Internet Crime Complaint Center (IC3), Annual Report 2024 (Apr 2025). $2.77 bn BEC losses globally in 2024.
9. Anthropic API Pricing Page (anthropic.com, accessed Jan 2026). Haiku 4.5: $1/$5; Sonnet 4.6: $3/$15; Opus 4.7: $5/$25 per M tokens.
10. Google AI Developer Pricing (ai.google.dev, accessed May 2026). Gemini 2.5 Flash: $0.30/$2.50; Flash-Lite: $0.10/$0.40 per M tokens.
11. Gartner Research, multiple reports cited via ChatMaxima AI Statistics 2026, Kodif AI Statistics (Nov 2025), Crisp Customer Service Impact (Apr 2026).
12. APCERT Annual Report 2024; Sitewall.net Cyber Threat Analysis 2022-24 (May 2025). 47% rise in CERT-In incidents.

THANK YOU

Let's continue the conversation.

Find me at the break — happy to walk through any of these in detail for your firm or your clients.

Rishabh Prakash

LinkedIn · /in/rishabhprakash

connect@rishabhprakash.com

Slides + detailed playbook in handout