IS Audit – Backbone to BFSI Industry

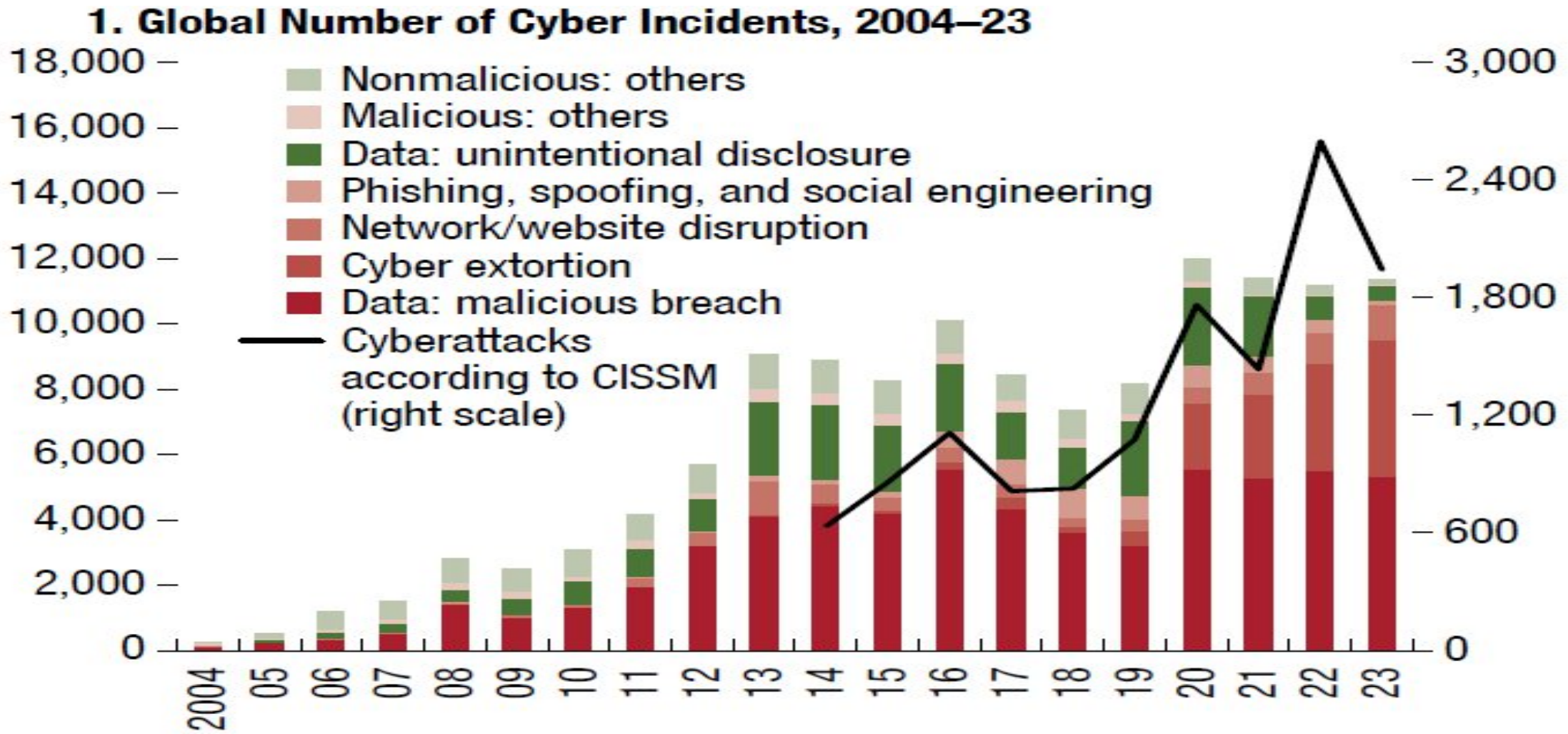
Ensuring secure and compliant financial operations

Sailaja Rani Jampala,
GM
CSITEG, DoS, RBI
May 22, 2026

Agenda

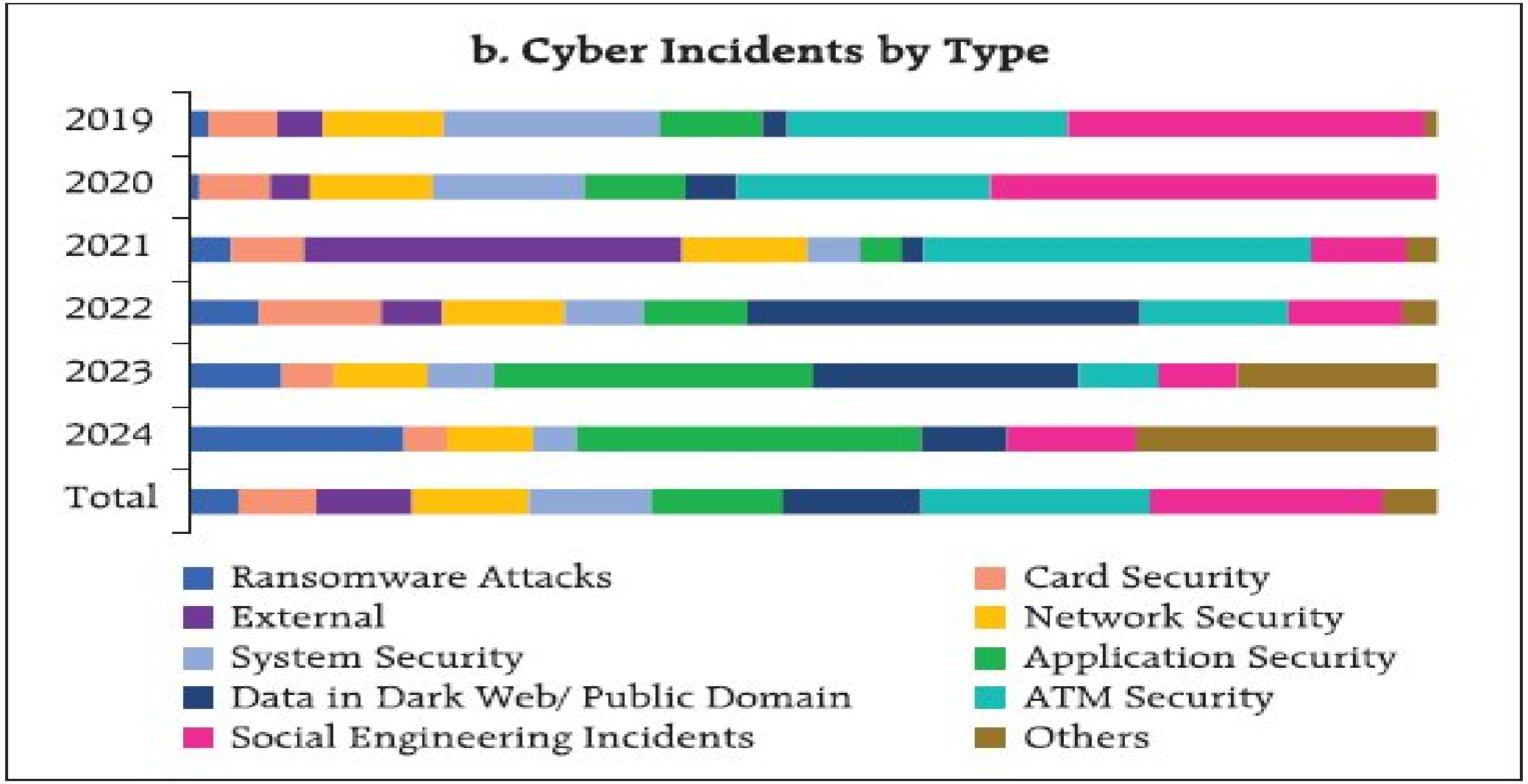
- Transformation of IS Audit in BFSI and Need
- Regulatory Evolution - Compliance to Resilience
- Continuous Assurance /Audit-as-a-Code
- Key Regulatory Frameworks
- Auditing Emerging Technologies
- Emerging Specializations
- Strategic Advisor Role
- Strategic Summary

IMF – Global Financial Stability Report (GSFR) Threat Landscape



Digital avenues facilitated as banking channels for banks and customers , at the same time the cyber incidents have grown exponentially

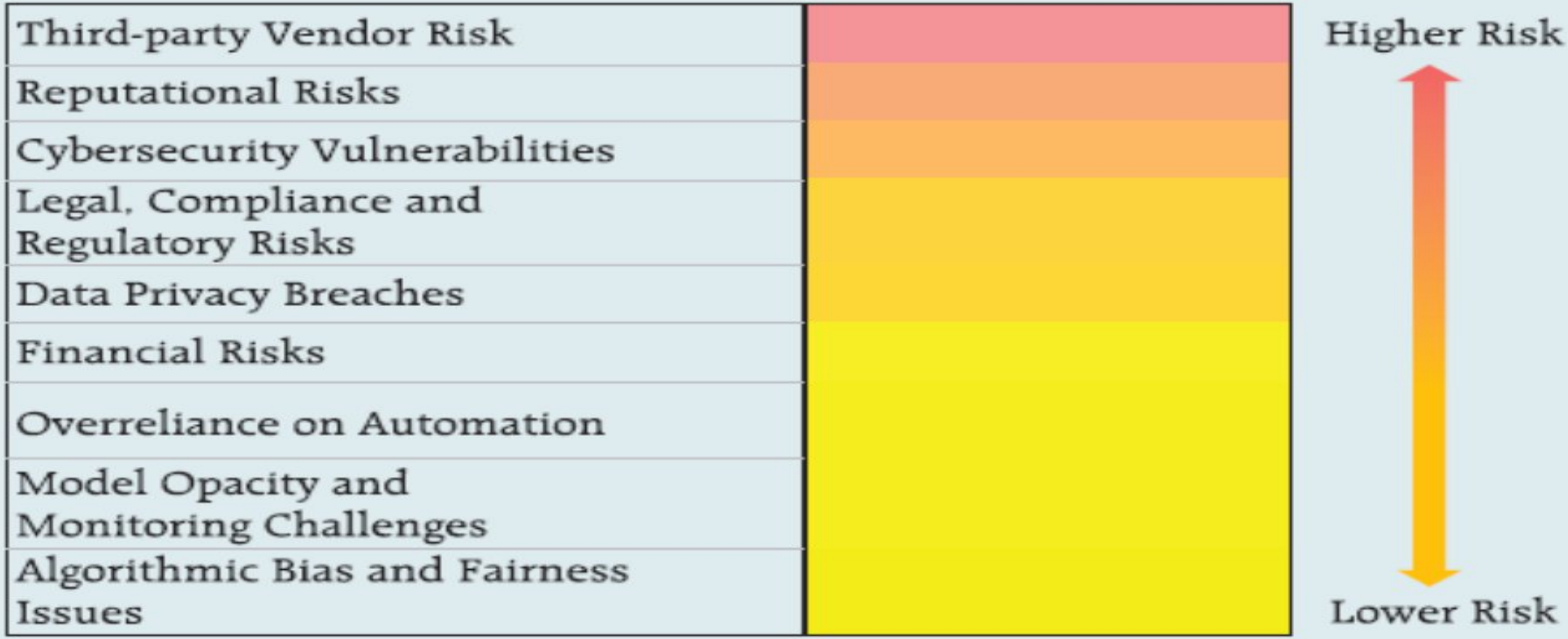
Overall picture of cyber incidents reported by SCBs, UCBs and NBFCs



FSR June 2024 Issue – Social engineering definition and cyber maturity of different types of SEs

Risks related to emerging technologies - FSR December 2024

b. Risks Identified in Adoption of AI/ML Technologies



Critical Risk Areas identified during ITE

- IT Governance
  - Inadequate Budget Utilization
  - Not comprehensively highlighting risk indicators / posture to Executive / Board Committees
  - Inadequate manpower in IS function.
- Data Governance
  - Lack of comprehensive Data Leak Prevention (DLP) strategy and processes
- Business Continuity and DR Drills
  - Non-conduct of DR drills for critical applications
  - Ineffective backup and restoration testing
- Capacity Management
  - The absence of a process to perform load testing, stress testing and capacity testing for public facing applications prior to their deployment
- Fraud Risk Management
  - Critical Applications not integrated with FRM
- Change and Vulnerability Management
  - Deficiencies in conducting security risk assessment of major changes
  - No Review of changes after implementation.
  - Delay in remediating vulnerabilities.
- Vendor Risk Management
  - Inadequate onboarding checks for vendors.
  - Lack of timely review of the vendor risk assessment framework
- Network Security including SOC
  - Inadequacies in network segmentation.
  - Use of vulnerable protocols such as Remote Desktop Protocol(RDP), PowerShell.
- IS Audit
  - Prolonged delays in addressing critical IS audit observations.
  - Lack of requisite resources or skillsets for IS Audit

Regulation and compliance Perspectives

Cyber Security Risk Governance

- User Access Management
- Network Security
- SOC & SIEM
- DB Security & DAM
- BCP/DR
- Fraud Risk Monitoring
- Cloud Security/ ATM Security/ Vendor Risk Management
- Capacity Management/ Inventory Management
- Non-Compliance to MDs
- Secure Configuration/ Patch Management / VAPT
- Advanced Real-time Threat Defense and Management/ Data Loss prevention
- Application Security Life Cycle- ASLC
- IS Audit

Practical Instance highlighting the role of IS Audit in Fraud Prevention

- Audit of Reconciliation process before making application live, based on which the frauds could have been prevented.
- One of the commercial bank lost approx. a two digit amount in crores of rupees, primarily considered due to not conducting thorough reconciliation implementation in a variant of UPI application rollout.
- One of the NBFC lost close to a two digit amount in crores of rupees (in less than 48 hours), primarily considered due to series of API related control weakness and conducting of reconciliation on T+2 basis.
- One NBFC lost money in a single digit of crores of rupees primarily due to vendor due diligence and other oversight weaknesses
- Fraud could be averted/loss minimized, if the IS Audit vertical (as third independent defense line) was involved before role out of new applications and ensuring that recon is conducted on real-time or near real-time basis.

Gaps in conduct of IS Audit

1. IS audit team was not looped in before new applications going live and before the critical applications undergoing major changes, as a result, Pre-Implementation audit was not performed by the IS audit team for the applications.
2. Actual posture of the IS audit findings was not projected/showcased to the Audit Committee of the Board and ACB's directions on the closure of the pendency of the findings was not maintained.
3. In some of the cases, VAPT was also performed/led by the IS audit team, whereas the IS audit team shall oversee the efficiency and pendency of the VAPT carried out by the Information Security team.
4. Periodic coverage of the IS audit (for the applications) based on the Audit calendar was not followed.
5. Huge pendency in closure of IS Audit observations beyond TAT defined (sometimes, we see pendency dating back 2 years too).
6. Limited strength of IS Audit team.

Transformation of IS Audit in BFSI

Evolving Risk Landscape

BFSI sector faces new risks like cyber threats, financial crime, and regulatory changes, demanding advanced audit approaches.

Real-Time Audit Requirements

Modern financial systems require continuous, real-time audit oversight due to fast transactions and cloud infrastructures.

Regulatory Expansion and Data Protection

Laws like DPDP Act expand IS Audit roles to include data protection, consent management, and breach governance.

Continuous Assurance Evolution

IS Audit is evolving into a continuous assurance function integrating AI, cloud, and emerging quantum risk management.

Need for Transformation

Technological Acceleration Impact

Rapid technological changes require IS Audit to adapt from static checks to real-time monitoring to manage emerging vulnerabilities.

Regulatory and Governance Evolution

New regulations like the DPDP Act demand stronger data governance, including data localization and breach notification frameworks.

Shift to Systemic Resilience

IS Audit must move from compliance to systemic resilience, embedding continuous assurance into financial architectures.

Regulatory Evolution

Shift to Operational Resilience

Regulators emphasize proactive frameworks focusing on operational resilience over retrospective compliance to strengthen institutions.

RBI and EU Regulatory Updates

India's RBI and EU's DORA regulations set standards for IT governance and critical service continuity amid technology disruptions.

Expanded IS Audit Responsibilities

IS Audit now requires deeper evaluation of real-time controls, vendor risks, and readiness for cyber incidents.

Adapting to Evolving Regulations

IS Audit teams must enhance technical skills and employ forward-looking methods to maintain compliance and effectiveness.

Compliance to Resilience

Limitations of Traditional Compliance

Traditional audits focus on policy verification and historical logs, which fail to address dynamic threats effectively.

Resilience-Oriented Auditing

Auditing now tests real incident responses, including failover, response times, and real-time detection capabilities.

Compliance–Resilience Gap

Many organizations meet compliance on paper but lack tested controls under real conditions, creating a critical gap.

Evolving Audit Responsibilities

IS Auditors must validate incident response, stress-test controls, and ensure anomaly detection for robust assurance.

Matrix Structure to ensure Effective comprehensive IS Audit

	Business Applications					Security Solutions				
	CBS	IB	MB	UPI	DLA	SIEM/SOC	DLP	DAM	NBAD	Firewall
BCP (DR Drill)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Backup & Restoration	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Capacity Management	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Patch Management	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Rule/Policy Review						Yes	Yes	Yes	Yes	Yes
Secure Configuration/Hardening	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Application Monitoring	Yes	Yes	Yes	Yes	Yes					
VA/PT	Yes	Yes	Yes	Yes	Yes					
Reconciliation of Transactions	Yes	Yes	Yes	Yes	Yes					
SOP Maintenance	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Governance (Roles/Responsibilities across teams)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Vendor Risk Management	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Regulatory Compliance	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
KRI/KPI Reporting to Top Management	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Cloud Security	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Change Management	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
User Access Management	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DPDP Act	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Inventory Management	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Auditing Emerging Technologies

AI Models

- The OWASP Top 10 for LLM Applications is the definitive framework for understanding security risks in modern AI agentic world.

- IS Auditor role is to ensure that all AI workflows or AI Agents are properly tested against these Top 10 vulnerabilities before making the agents live.

- Use the latest OWASP Top 10 lists that will released every year to validate the AI applications.

Role of IS Audit in DPDP Rule Implementation

Role of Auditor in implementation and sustenance of compliance to ‘Rule 6’

1) Ensure implementation of Aadhar Data Vault.
2) Ensure clear definition of PII data fields in policy.
3) Ensure that PII data fields are masked/encrypted at Database level.
4) Implement Security tools related to Data Security like DLP, DAM, Data Classification.
5) Ensure integration of DLP, DAM solution logs to SIEM and creating appropriate rules at SIEM.
6) Data backups & Restoration testing
7) Apart from these specific Data security controls, controls at Perimeter/Network, End-point, Applications etc needs to be ensured.

Strategic Summary

- Increasing the strength of IS Audit team- quality and quantity
- Continuous IS Audit
- Technological Integration
- Developing expertise among IS Audit team members across core security domains like Application Security Testing, Network Security, Cloud Security, Container Security, API security, Database Security, AI/ML deployments etc.
- Strategic Assurance Role

Thank you

Sailaja Rani Jampala,
GM
CSITEG, DoS, RBI

IS Audit – A Backbone to BFSI industry

Industry need and expectations due to teach adoption

Digital Transformation Finance Summit (DxFS) 2026, ICAI, Hyderabad

May 22, 2026

About me (“the presenter”)

CA Vishal Saraswat

- Having an overall 19+ years of experience in risk management, information systems and cyber security audits, data analytics, vulnerability management.
  - Worked as Head - IS Audit for four years in ICICI Bank (*till March 2026*)
  - Currently responsible for Vulnerability Management of ICICI Bank and its international banking subsidiaries.

- Qualification and certification: CA, CISSP, CISA, CCSP, CCSK, CEH, CNSS, ISO-27001, Independent Director, SAS, Python, etc.
- Currently persuing MCA (Masters in Computer Application)

CA – Chartered Accountant
CISSP – Certified Information Systems Security Professional
CISA – Certified Information Systems Auditor
CCSP – Certified Cloud Security Professional
CISA – Certified Information Systems Auditor
CCSK – Certificate of Cloud Security Knowledge

Disclaimer:

Any views or opinions expressed as part of this presentation are solely of the presenter's and do not represent those of ICICI Bank.

Agenda

A Few Qualities…

IS Audit: Coverage

Why IS audit looks complicated

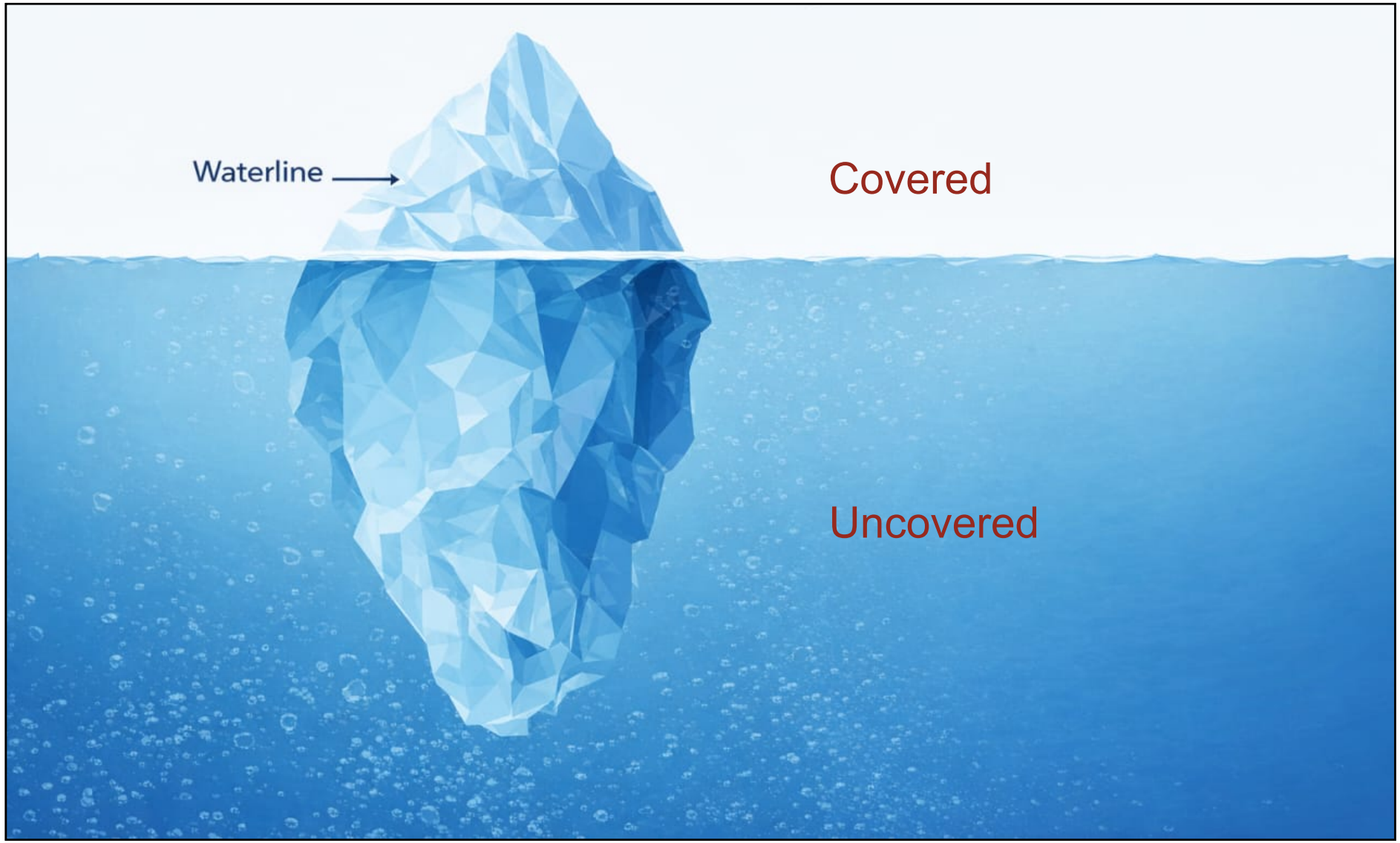
Key expectations

Key challenges

Few key qualities…

- Business Understanding
- Logical thinking / Integrated thinking
- Risk correlation ability
- Strong analytical skills
- Attention to detail
- Problem solving skills

IS Audit coverage



Why IS Domain looks comp

How to simplify

- Structured and logical thinking
- Avoid Ad-hoc understanding
- Join dots to understand complete universe
- Apply common sense
- Clear understanding of risk and controls environment
- Understand how security controls works
- Enjoy Technology & Security

Key expectations

Single end-to-end package

- Risk Management
- Data Analytics
- Business Understanidng
- Technology
- Security & Data Privacy

Technical and data driven

- Risk Based ITGC audits
- Application threat modelling
- Security controls weakness
- Security controls by-pass
- Using AI to perform audits

Agile audits / assessments

- Move out from process compliance audit
- Application threat modelling
- Red Teaming Activity
- Focus on real risk
- Scenario based audits

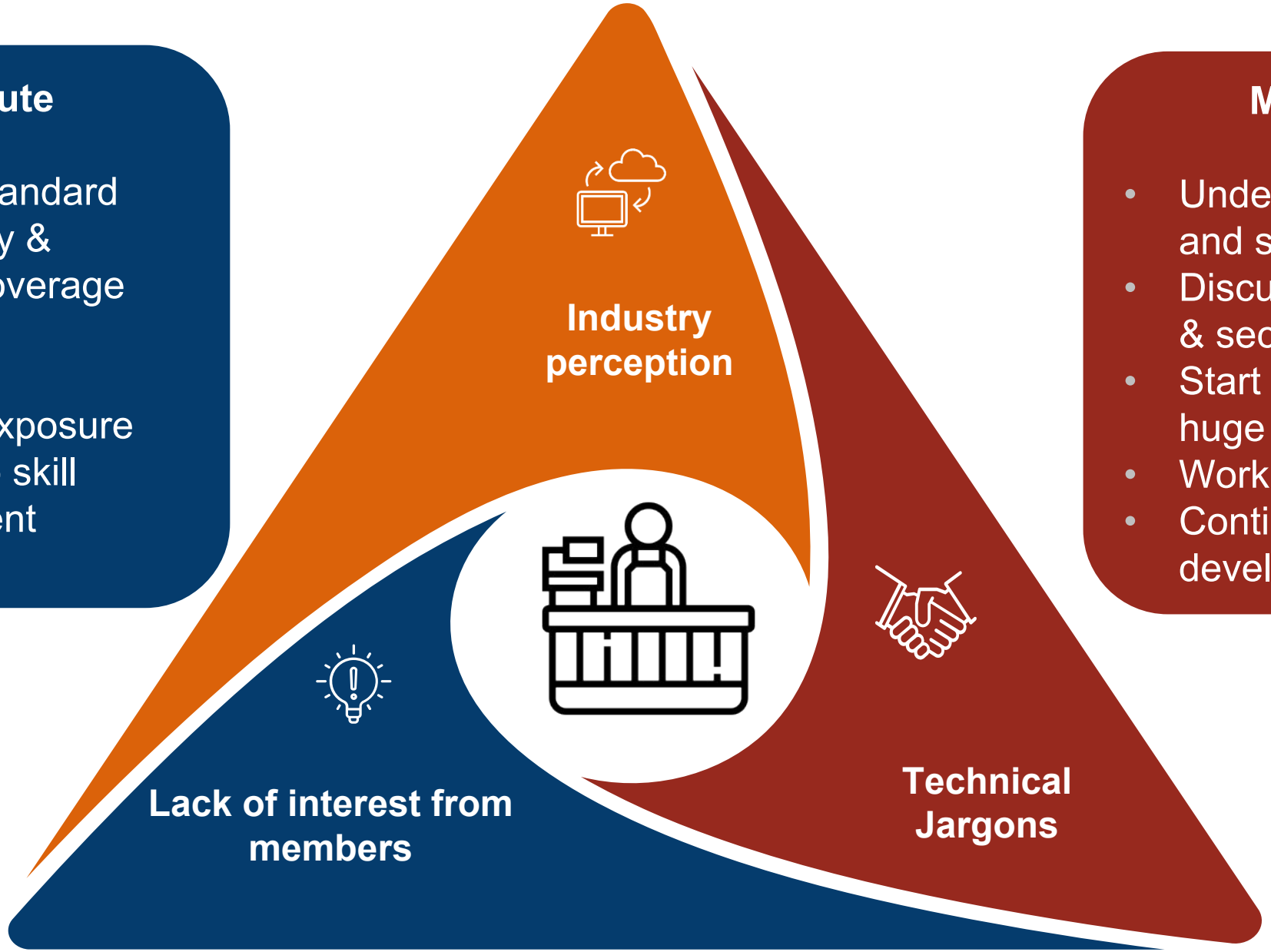
Advisory / problem solving

- Regulatory guidelines implementation
- International Regulation
- Frameworks
- New Attack (Mythos)
- Software development

Key challenges

Institute

- IS Audit Standard
- Technology & Security coverage
  - DISA
  - CA
- Practical exposure
- Platform to skill development



Members

- Understand in letter and spirit
- Discussion technical & security aspects
- Start working on huge opportunity
- Work from today
- Continuous skill development

Thank you

Where Technology Meets Assurance

Evolving Practice Areas for the IS Auditor

CA. R. Vittal Raj

JULY 2024

Banks and payments hit as faulty CrowdStrike update causes

UPI hits record scale: 24,162 crore transactions worth ₹314 lakh crore in FY26

The government reiterated its commitment to strengthening the digital payments ecosystem, with a focus on innovation, security, and inclusion, as UPI continues to scale new milestones

Published – May 01, 2026 11:25 am IST – New Delhi

Source: Microsoft, Parametrix, CrowdStrike PIR (2024)

"Man stands in his own shadow and wonders why it's dark."

Zen

When Computers met Banking..

When RBI started regulating IT Risk..

When Banks went Digital..

When Customers are demanding Digital Trust..

Banking has gone Digital…Customers have gone digital…Regulators have gone Digital…. Have we matched instep……

Did IS Audit evolve?

Are we assuring on Digital Trust?

Japanese Teens Arrested for Using ChatGPT Contract

March 4, 2025

Gen Z faces 'job-pocalypse' as global firms prioritise AI over new hires, report says

Banks On Edge, Finance Ministry On Alert: Mythos AI Panic Explained

Mythos, an advanced AI model developed by Anthropic, can compress weeks of hacking effort into hours. This is making banks nervous globally.

Edited by: Prateek Shukla | Business News | May 06, 2026 07:04 am IST

ARTIFICIAL INTELLIGENCE

Hackers Weaponize Claude Code in Mexican Government Cyberattack

The AI was abused to write exploits, create tools, and automatically exfiltrate over 150GB of data.

By Ionut Arghire | March 1, 2026 (7:30 AM ET)

For three centuries we audited *the ledger*.

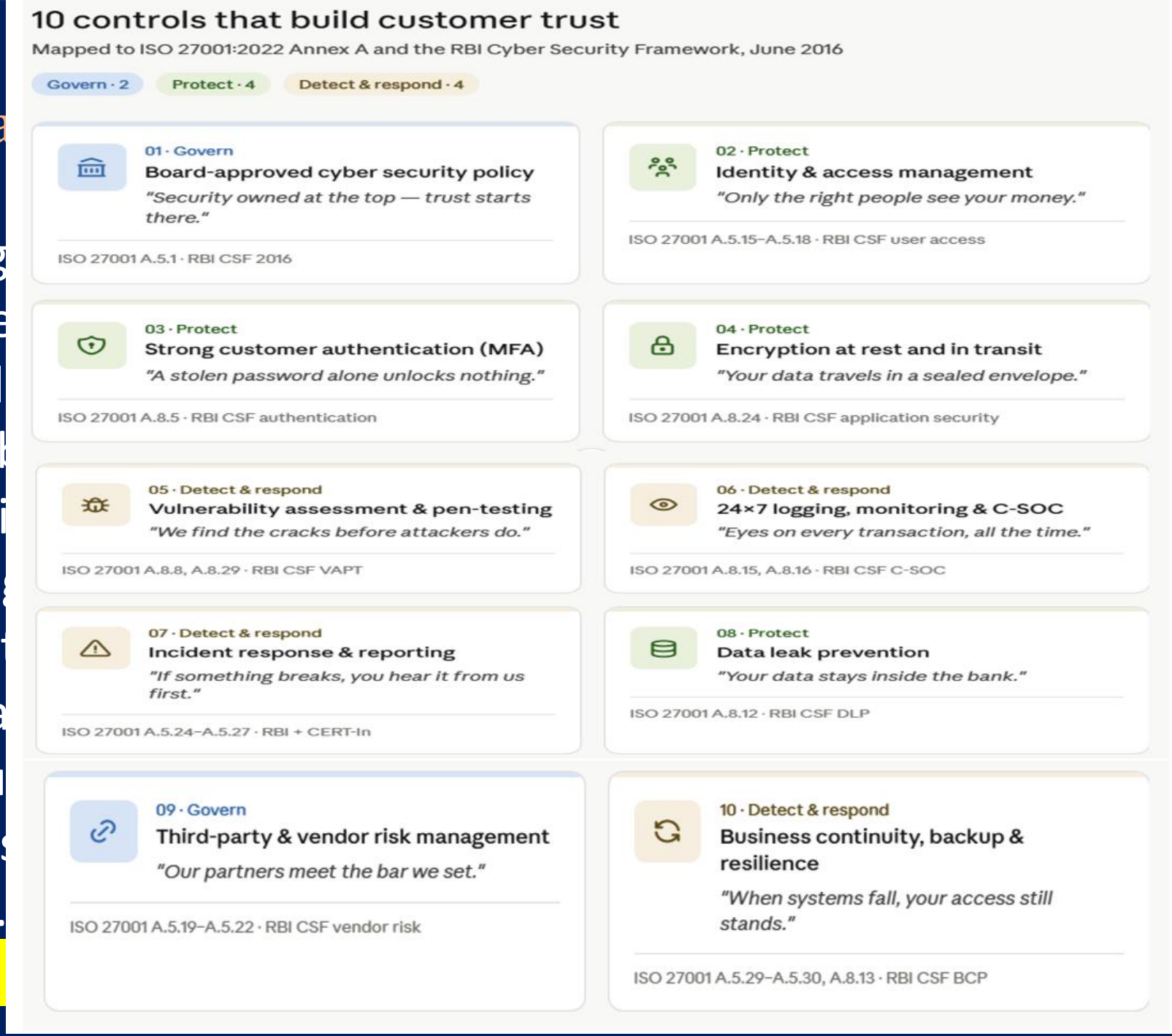
For thirty years we audited *the logic behind the ledgers*.

Today we must audit *the intelligence, the infrastructure, and the third parties* that decide what the ledger says.

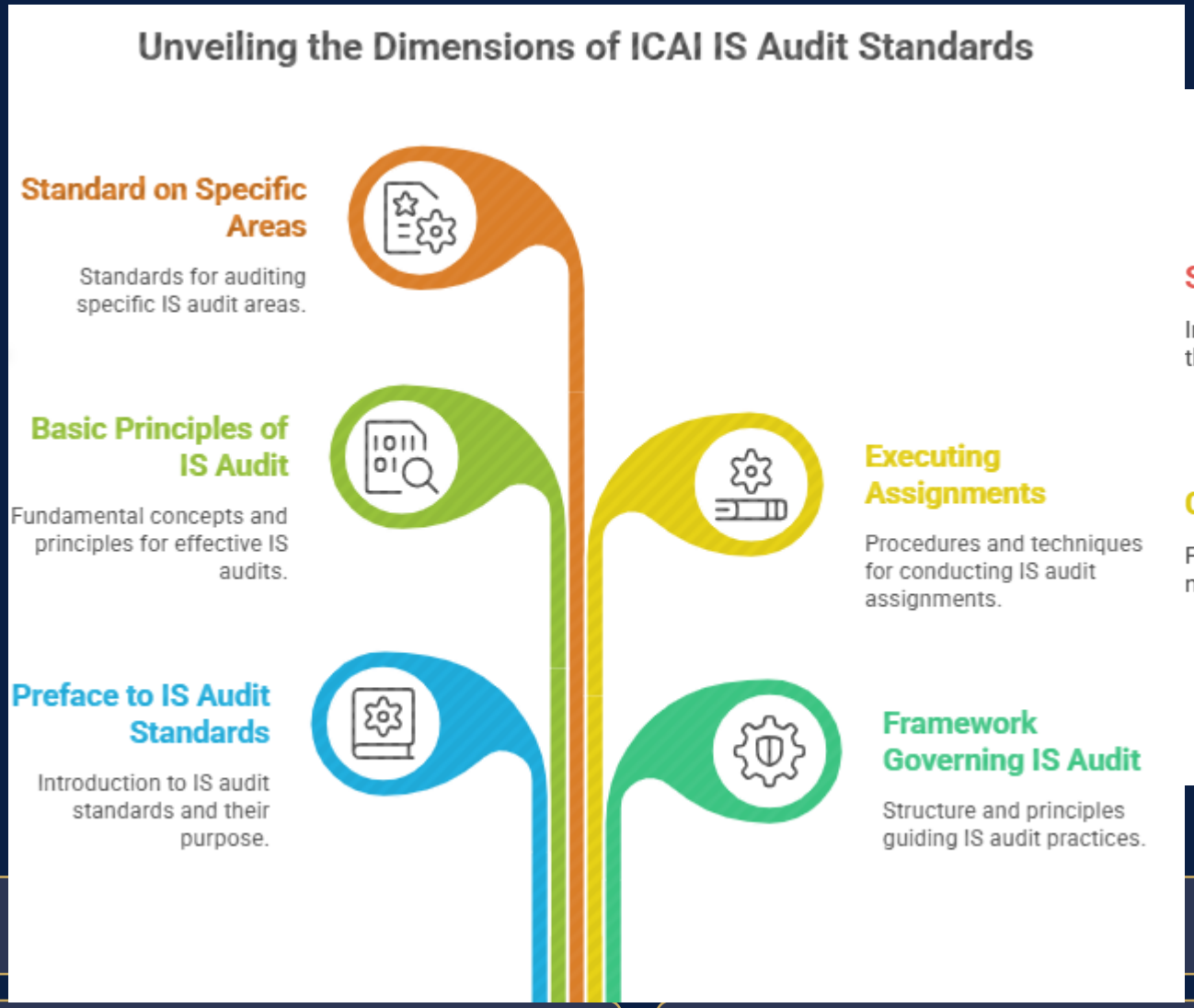
Assurance has moved from the back office to the engine room.

Why IS Auditors a

- Contextual thinking
- When a LOS App de
- When an audit trail
  technically correct
  looking at audit trai
- When an AI model
  unknown fraud patt
- Regulatory Complia
- A customer in genu
- When dark pattern
- And now Mythos....
- Moving from auditi



• Practice Areas that are already lookin



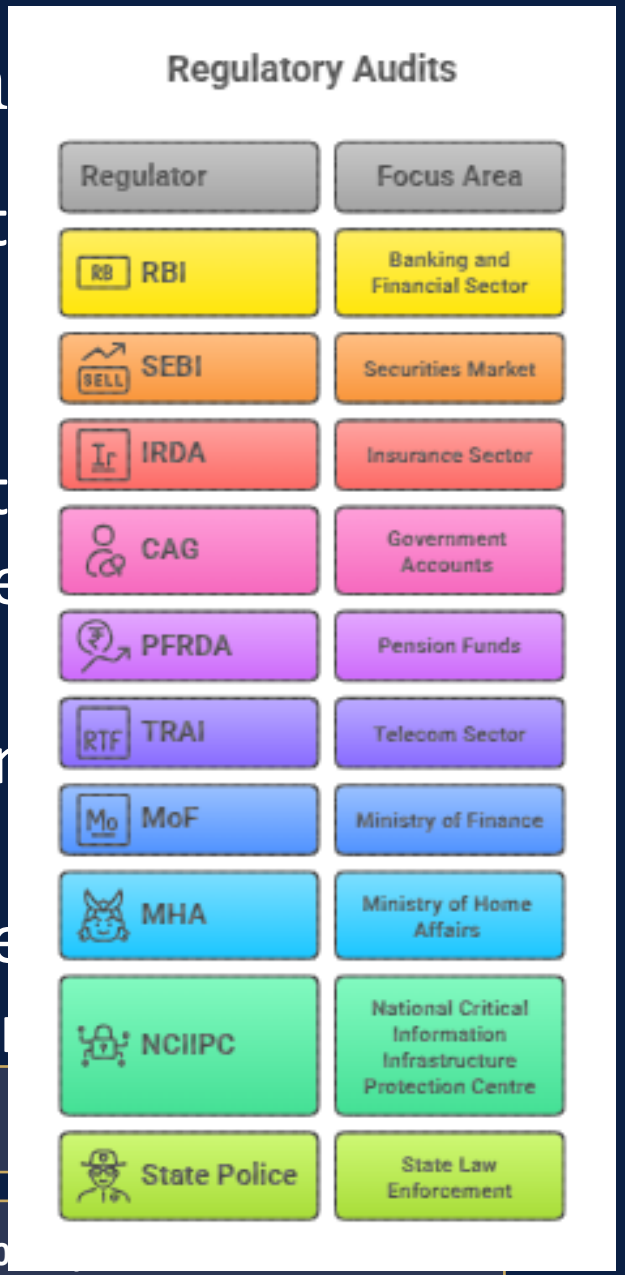
Self-Governance Driven

Internal policies, not external threats

Compliance Driven

Focus on regulations, not business needs

autonomous



03

04 Third-Party & Supply Chain

05 DPDP Assurance

The Future is not what it used to be!

- Agentic AI & Domain specific LLMS - autonomous agents that decide, transact, reconcile, close transactions by themselves.
- BFSI dissolved into commerce platforms
- Open banking and Account Aggregator consent-driven rails.
- CBDC and programmable money
- Quantum Risks and the scare of PQC and harvest-now-decrypt-later attacks
- AI security and governance platforms for logic control
- Next level Deepfakes
- AI-native wearables and ambient voice-led banking

Whatever the Technology, Fundamental Audit Questions remain the same – Is it Trustworthy | Doing what it is supposed to do?| Not doing what it is not supposed to do|

Before Closing

The tools change.

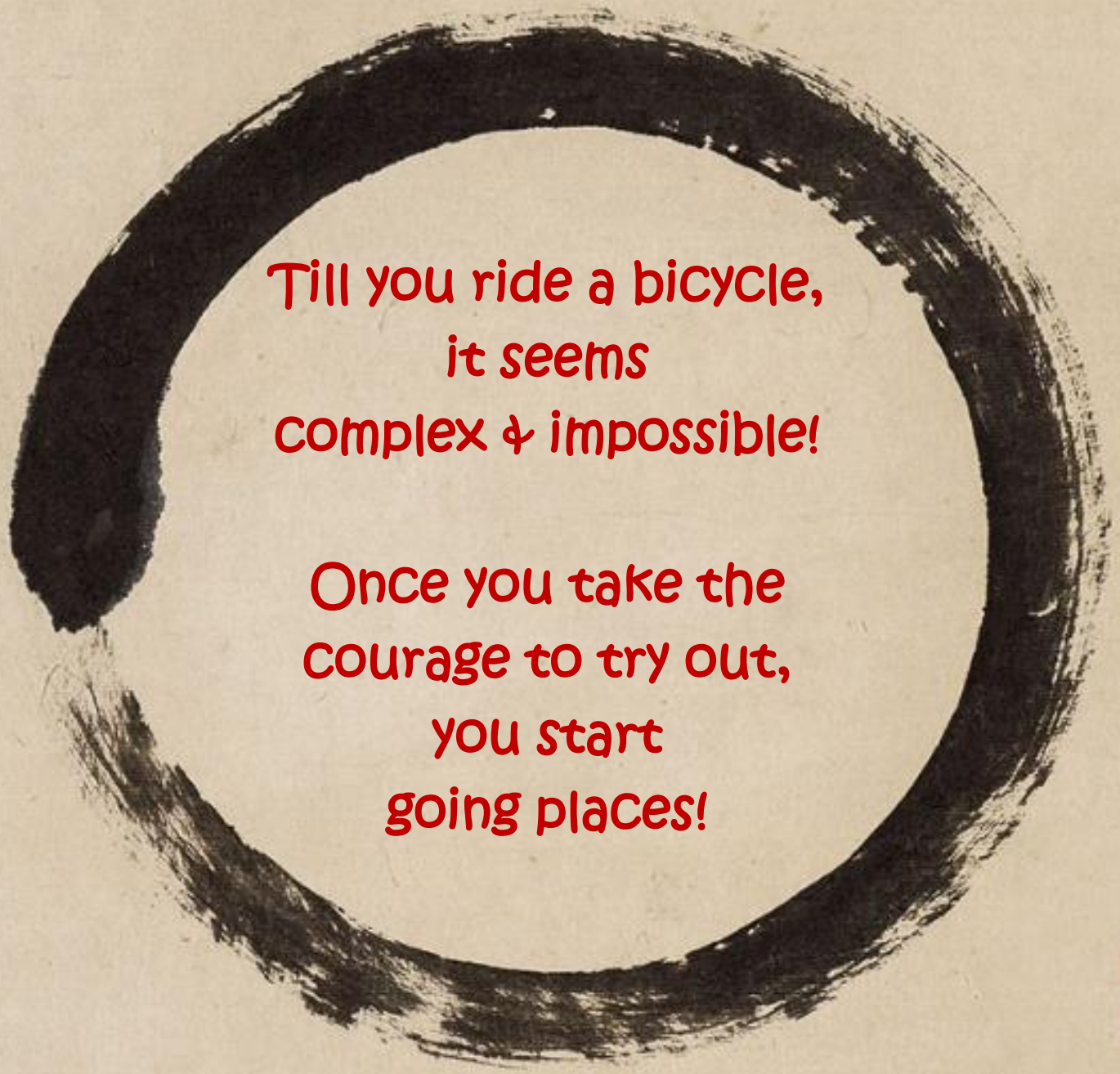
The question we are paid to answer does not.

Can we stand up to the trust in is?

Someone in every institution must have the standing, the skill, and the spine to say — ***not yet.***

That someone is us!

A CA armed with Business Technology Competence is the best IS Auditor! Take that leap today!



Your own Self-realization is the greatest service you can render the world !

Thank You !!!

R Vittal Raj,

Kumar & Raj CAs

vittal@krca.in

Linkedin: r vittal raj

Enhancing Cyber Security in India

Securing the Digital Enterprise
–
Government Initiatives & Perspective

Abhishek Solanki| Scientist

Indian Computer Emergency Response Team (CERT-In)

Ministry of Electronics and Information Technology (MeitY)

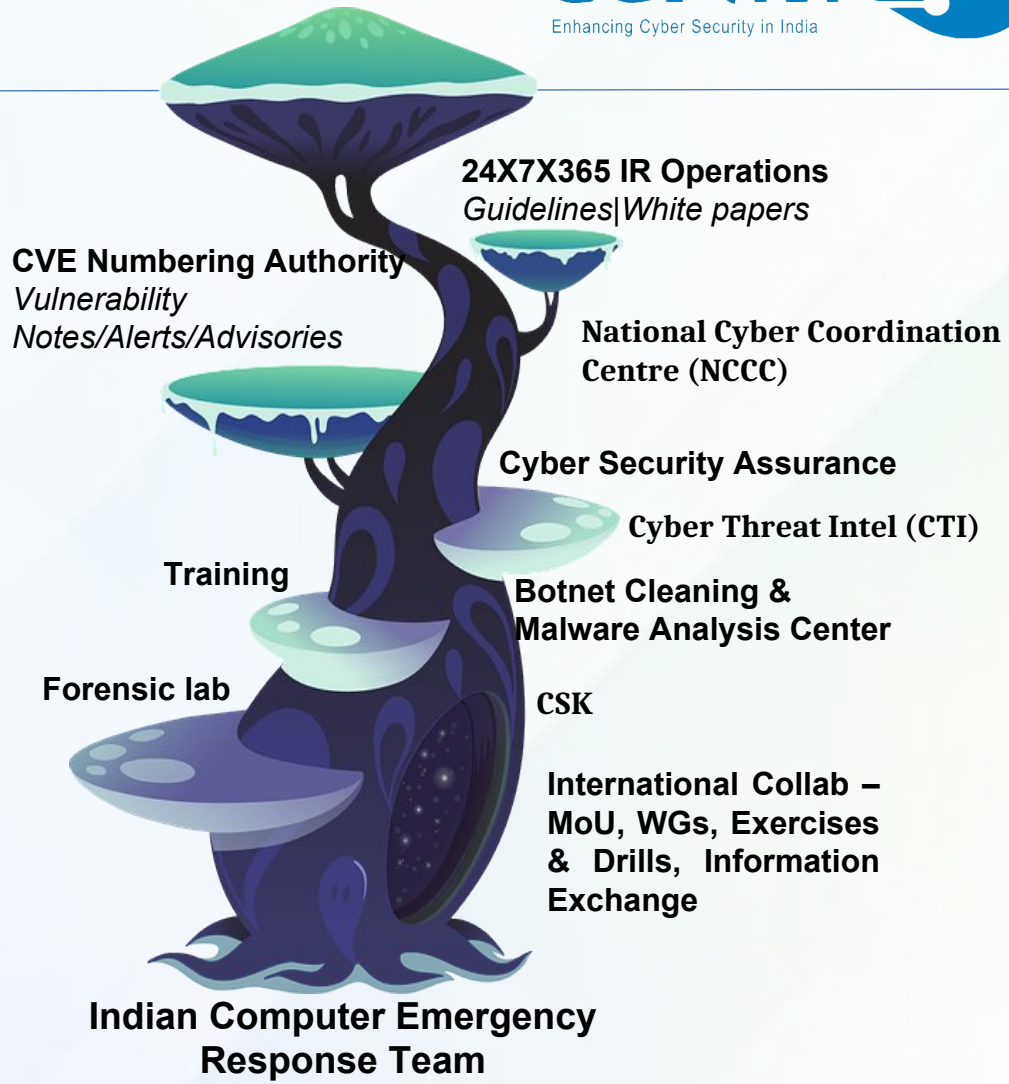
About CERT-In

To serve as the national nodal agency to perform Cybersecurity functions & services.
CERT-In is under the Ministry of Electronics and Information Technology, Government of India.

CERT-In is involved with Responding to cyber attacks to minimize Impact and reducing recovery time; proactive actions to minimize the national vulnerability to cyber attacks; Capacity building & enhancing cyber awareness among citizens; Provide Cyber security quality assurance

Constituency: Indian Cyber Community

Vision: Proactive, Reactive & Assurance Services for securing Indian cyber space



Mission: To enhance the security of India's ICT infrastructure through proactive action and effective collaboration

CERT-In Journey: Technical Organisation for Incident Response to Strategic Cyber Governance

Enhancing Cyber Security in India

In 2025, CERT-In handled 1 incident every 10 seconds

98% digital population covered by Cyber Swachhta Kendra. 1,427 organisations onboarded, and 89.55 lakh malware removal tool downloads.

237 empanelled cybersecurity audit organisations strengthened Audit & Assurance Ecosystem.

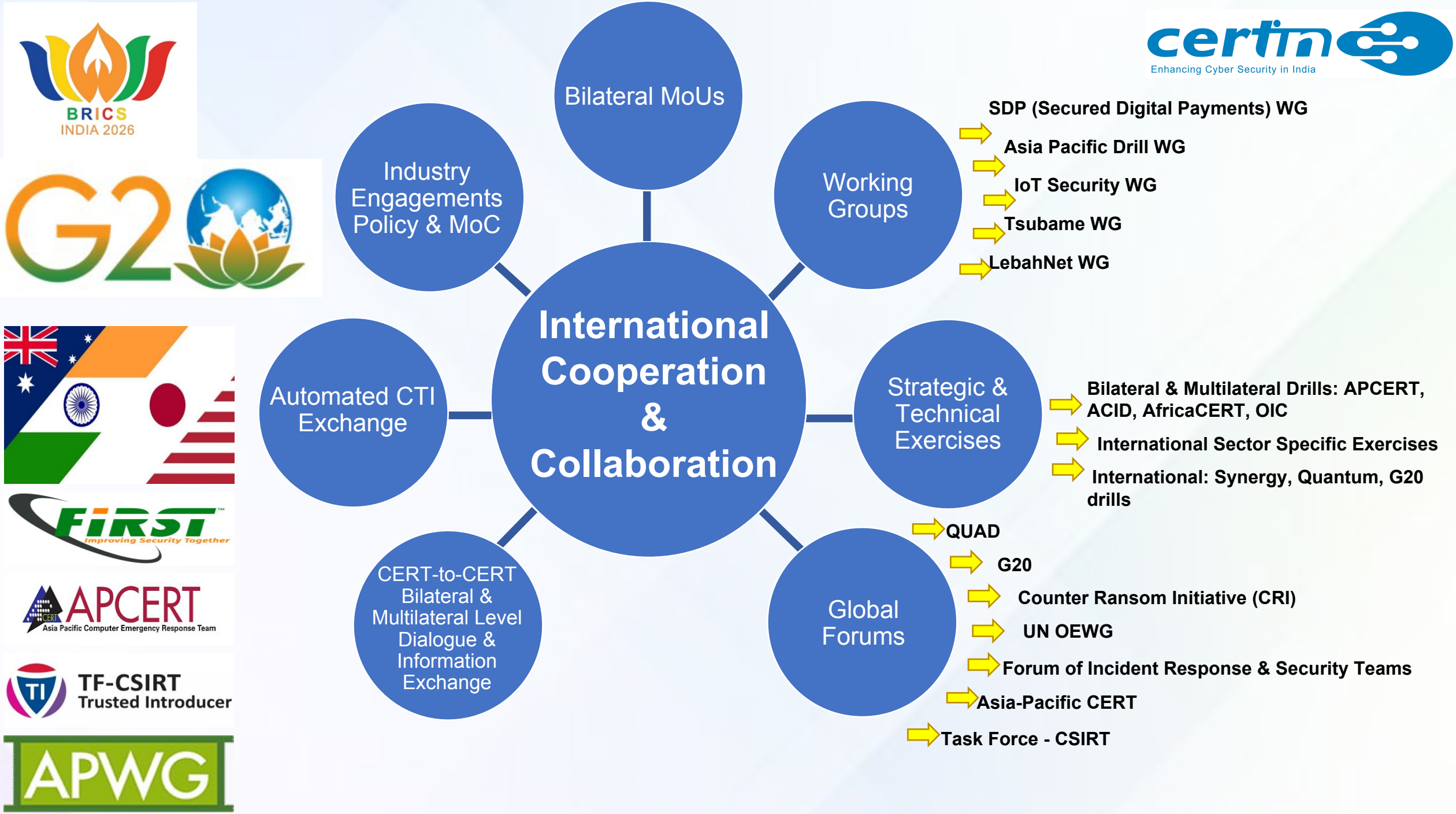
Technical Risk -> Business Risk, Capacity Building of Board Members, Shifting Right, Tactical and Strategic Controls

Year 2025- Issued over 5 alerts / advisories / vulnerability notes per day, reflecting large-scale national cyber response capability.

Global – ANSSI, GGEF-SBOM, WEF and Oxford for AI-driven threat detection and cyber resilience leadership.

India Cyber Defence Architecture: How CERT-In is quietly securing a billion user digital infrastructure

India's digital ecosystem expands at unprecedented scale, cybersecurity has emerged as a pillar of economic stability and governance. At the centre of this architecture, CERT-In has evolved into the institutional backbone securing India's digitally dependent economy


certin
Enhancing Cyber Security in India
BRICS
INDIA 2026
G20
FIRST
Improving Security Together
APCERT
Asia Pacific Computer Emergency Response Team
TF-CSIRT
Trusted Introducer
APWG
International Cooperation & Collaboration
Bilateral MoUs
Industry Engagements Policy & MoC
Working Groups
SDP (Secured Digital Payments) WG
Asia Pacific Drill WG
IoT Security WG
Tsubame WG
LebahNet WG
Automated CTI Exchange
Strategic & Technical Exercises
Bilateral & Multilateral Drills: APCERT, ACID, AfricaCERT, OIC
International Sector Specific Exercises
International: Synergy, Quantum, G20 drills
CERT-to-CERT Bilateral & Multilateral Level Dialogue & Information Exchange
Global Forums
QUAD
G20
Counter Ransom Initiative (CRI)
UN OEWG
Forum of Incident Response & Security Teams
Asia-Pacific CERT
Task Force - CSIRT

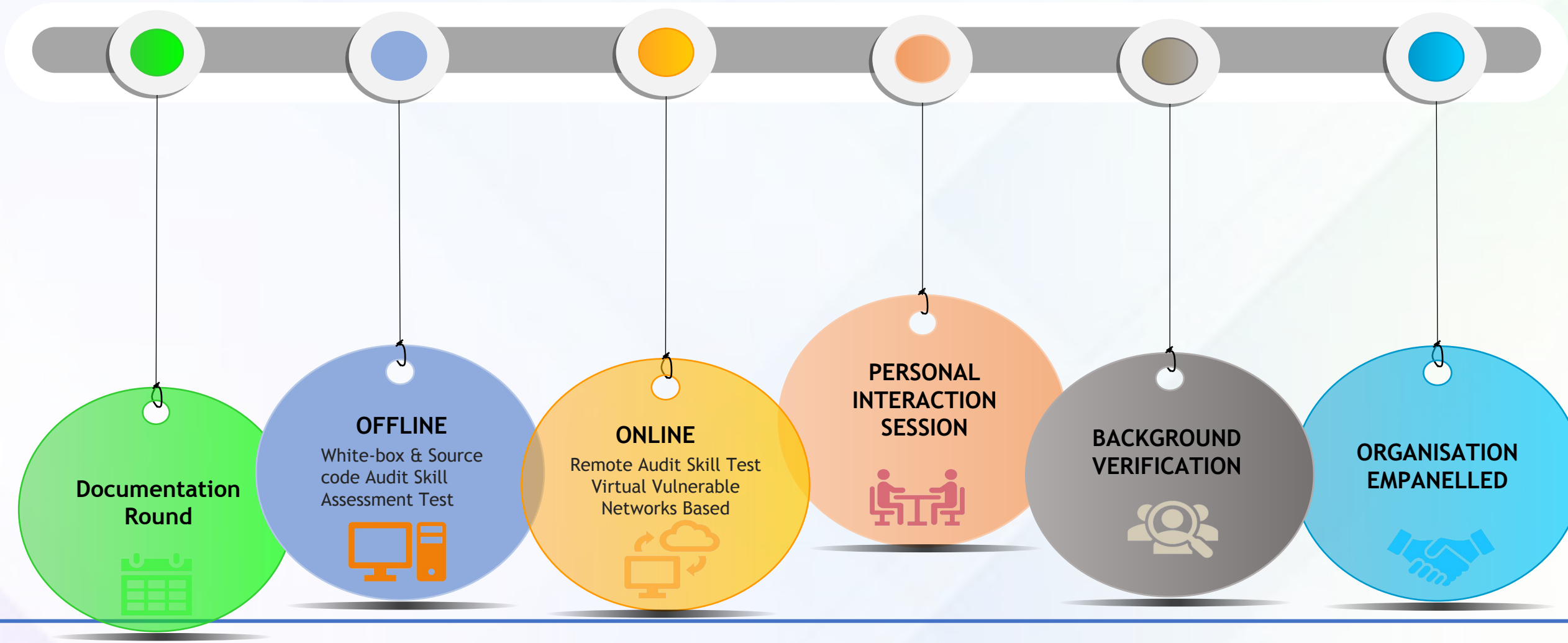
Snapshot of Activities and Incidents handled

Security Incidents	Numbers
Vulnerable Services	9,41,592
Unauthorized Network Scanning /Probing	4,47,720
Virus/ Malicious Code	1,84,131
Website Defacements	10,665
Website Intrusion & Malware Propagation	1,045
Phishing	869
Others	6,895

Activities	Numbers (January 2025 to December 2025)
Incidents handled	29,44,248
Security Alerts Issued	1530
Advisories Issued	65
Vulnerability Notes Issued	390
Training Programs & participants	32 Programs (Trained 20,799 participants)
International cyber security drills/exercises	05
Domestic Cyber security drills/exercises	18
Awareness sessions	78 Sessions (covers 91,265 participants)

Cyber Security Audits Landscape

Empanelment - Assuring Quality Cyber Security Auditing



Objective – Quality Cybersecurity Audits

CERT-In Initiatives to Strengthen the Audit Ecosystem

1. With multi-stakeholder consultations, CERT-In has developed and issued the "Comprehensive Cyber Security Audit Policy Guidelines“.
2. Developed and launched the Audit Monitoring, Benchmarking, Analysis and Kinetic Interventions (AMBAK) – Blockchain based platform.
3. Continuous Performance Evaluation of Empanelled Auditing Organizations - Enable & Understand and Deter & Punish Framework.
4. Development of advisory & guidelines based on the interaction with stakeholders and analysis of audit metadata & audit reports.
5. National Annual Conference “CERT-In SAMVAAD” for empanelled auditing organisations.

CERT-In SAMVAAD Annual Conference 2026

- **CERT-In** has organized 3-day **National Annual Conference "CERT-In SAMVAAD 2026"** on the theme '**Securing Digital Bharat through Future Ready Audits: Adapting, Assuring, Advancing**' to Strengthen India's Cybersecurity Audit Ecosystem.
- More than **200 paper submissions** received of which **87 presentations** selected.
- **Focus Areas:**
  - AI driven cyber risks such as emerging frontier AI models with advanced cyber capabilities
  - Emerging tools for automated audits
  - Blockchain and Post Quantum Cryptography (PQC)
  - SBOM, CBOM, QBOM, AIBOM and HBOM considerations
  - AI driven red teaming methodologies
  - Supply chain audits
  - UAVs, Drone, Space and Satellites cybersecurity
  - Innovative approaches to securing complex environments such as cloud systems, APIs and Operational Technology
- **Participants:**

  500 delegates, including Cybersecurity Auditors, Start-ups, Chief Information Security Officers (CISOs) and Regulators

Comprehensive Cyber Security Audit Policy Guidelines

Comprehensive Cyber Security Audit Policy Guidelines

Indian Computer Emergency Response Team (CERT-In)
Ministry of Electronics and Information Technology
Government of India

Version 1.0 | 25.07.2025

Table of Contents

"Guidelines are designed to align with the phases of the audit. By following this structured approach, both Auditee and Auditing Organizations can easily navigate through each stage of the audit process with a clear understanding of the required

Guidelines for Auditing Organizations (Key Points)

- Audit standards and Methodologies
- Background Verification of Auditors
- Specify the tools used for conducting audits in report
- Audit Team details in report
- Continuous capacity building of auditors
- Maker-Checker Concept to ensure Quality
- Handling of High-Risk Vulnerabilities
- Verification of Compliance to CERT-In & Regulatory Guidelines
- Audit Report Format
- Quality Audit Reports
- Security Gap Analysis Report
- Handling Audit related Data
- Revalidation and Follow up Audits
- Maintaining Updated Information with CERT-In
- Accountability for Audit Lapses and Adverse Feedback

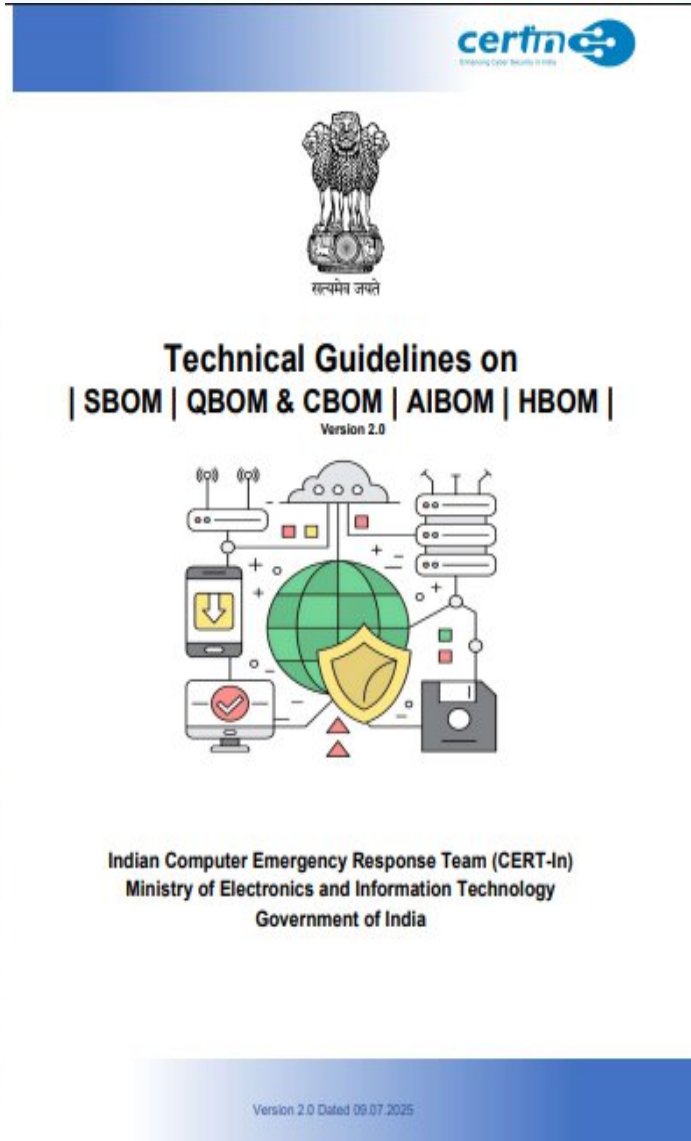
Guidelines for Auditee Organizations (Key Points)

- Audit Frequency
- Key Considerations for Comprehensive Audit Scope
- Comprehensive Asset Inventory
- Non Disclosure Agreement
- Ensuring Independent Audit Assessments
- Version Control and Change Management of audited application
- Use of Snapshot Information of auditing organisations
- Exceptions and Risk Acceptance of reported vulnerabilities
- Compliance with CERT-In & Regulatory Guidelines
- Audit of Critical databases/applications
- Adherence to SSDLC Guidelines of CERT-In
- Continuous Internal Audits/Assessments
- Feedback on the Audit to CERT-In
- Secure Handling of Report and Data
- Management Oversight in Audit Programs

Technical Guidelines on SBOM, QBOM, AIBOM and HBOM

- The guidelines address growing software supply chain security risks from third-party and external components.
- Targeted at government, public sector, essential services, and software/hardware/AI solution providers.
- Promote integrating BOMs into the procurement, development, and operations lifecycle to enhance resilience against cyber threats.

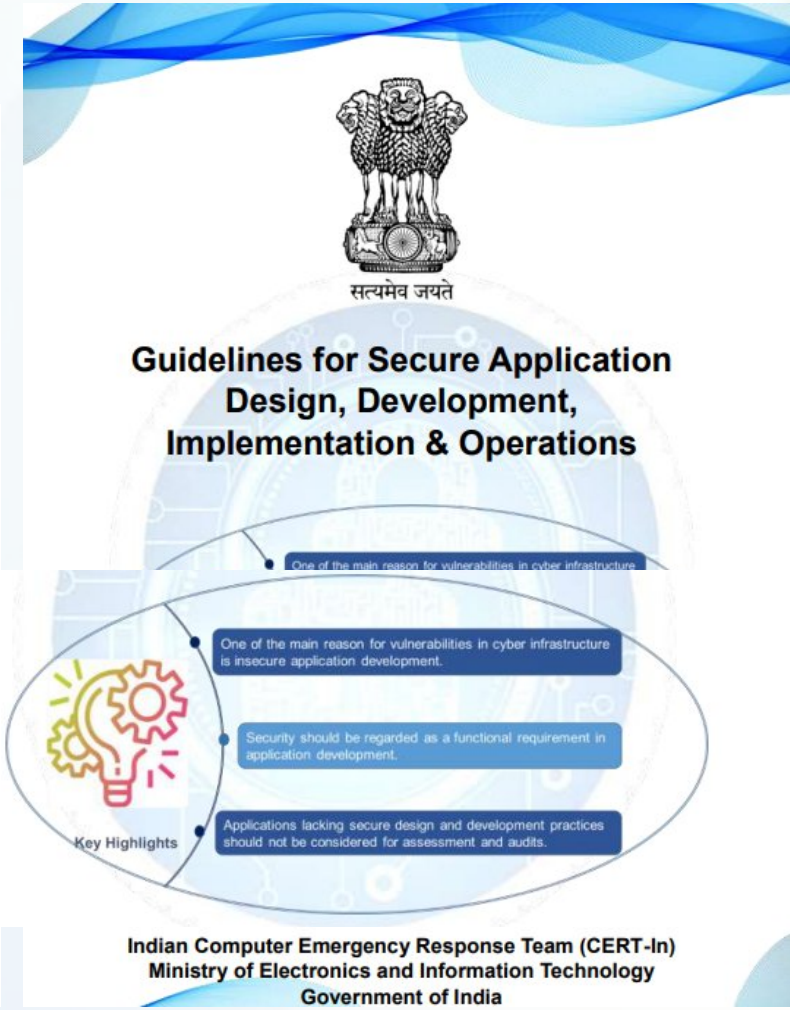
Table of Contents



Guidelines for Secure Application Design, Development, Implementation & Operations

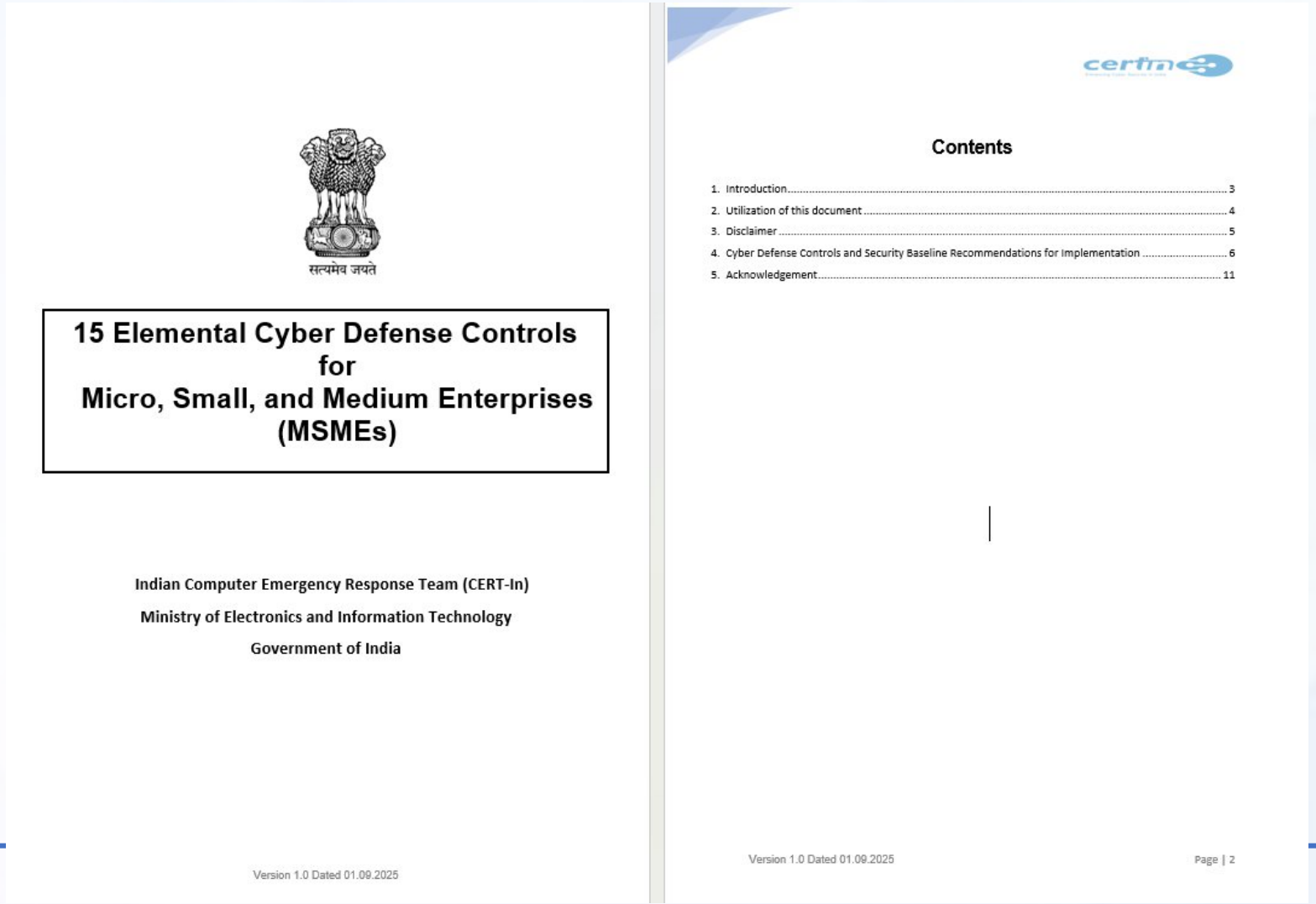
- **Security by Design** – Integrate security from inception using Secure SDLC frameworks.
- **Secure Development** – Apply strong authentication, encryption, coding best practices, and threat modelling.
- **Audit & Testing**
- **Deployment & Ops** – Ensure secure configs, continuous monitoring, timely patching, and supply chain risk control.

Table of Contents



15 Elemental Cyber Defense Controls for MSMEs

certin
Enhancing Cyber Security in India



सत्यमेव जयते

15 Elemental Cyber Defense Controls for Micro, Small, and Medium Enterprises (MSMEs)

Indian Computer Emergency Response Team (CERT-In)
Ministry of Electronics and Information Technology
Government of India

Version 1.0 Dated 01.09.2025

certin

Contents

- ✓ The document outlines 15 Elemental Controls of Cyber Defense along with 45 security baseline recommendations mapped to these controls specifically designed to guide MSMEs in strengthening their cybersecurity posture.
- ✓ These controls serve as baseline cybersecurity criteria.
- ✓ MSMEs can initiate their journey toward a comprehensive cybersecurity framework in a structured and practical manner.

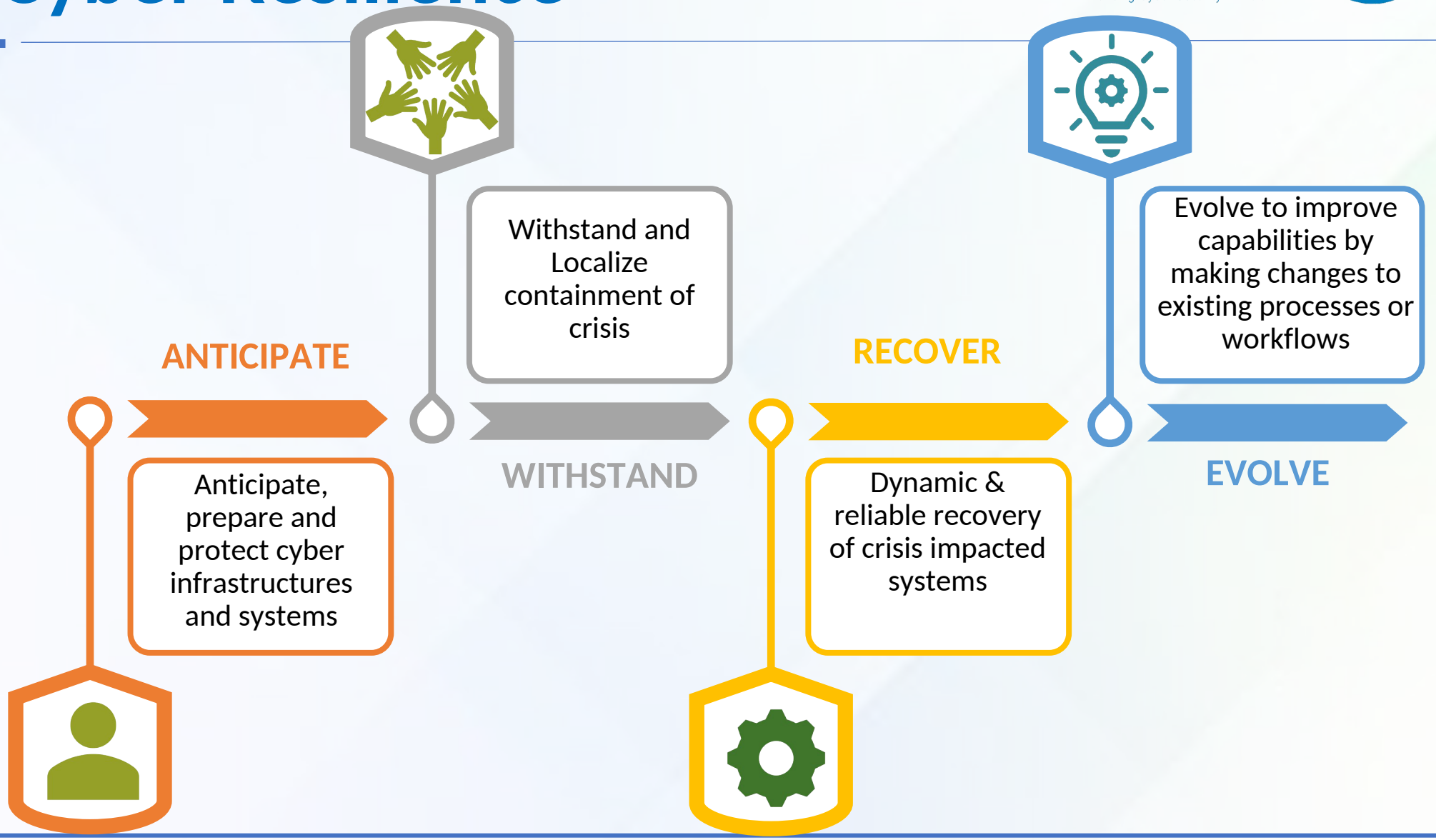
Security to Resilience

Towards Cyber Resilience

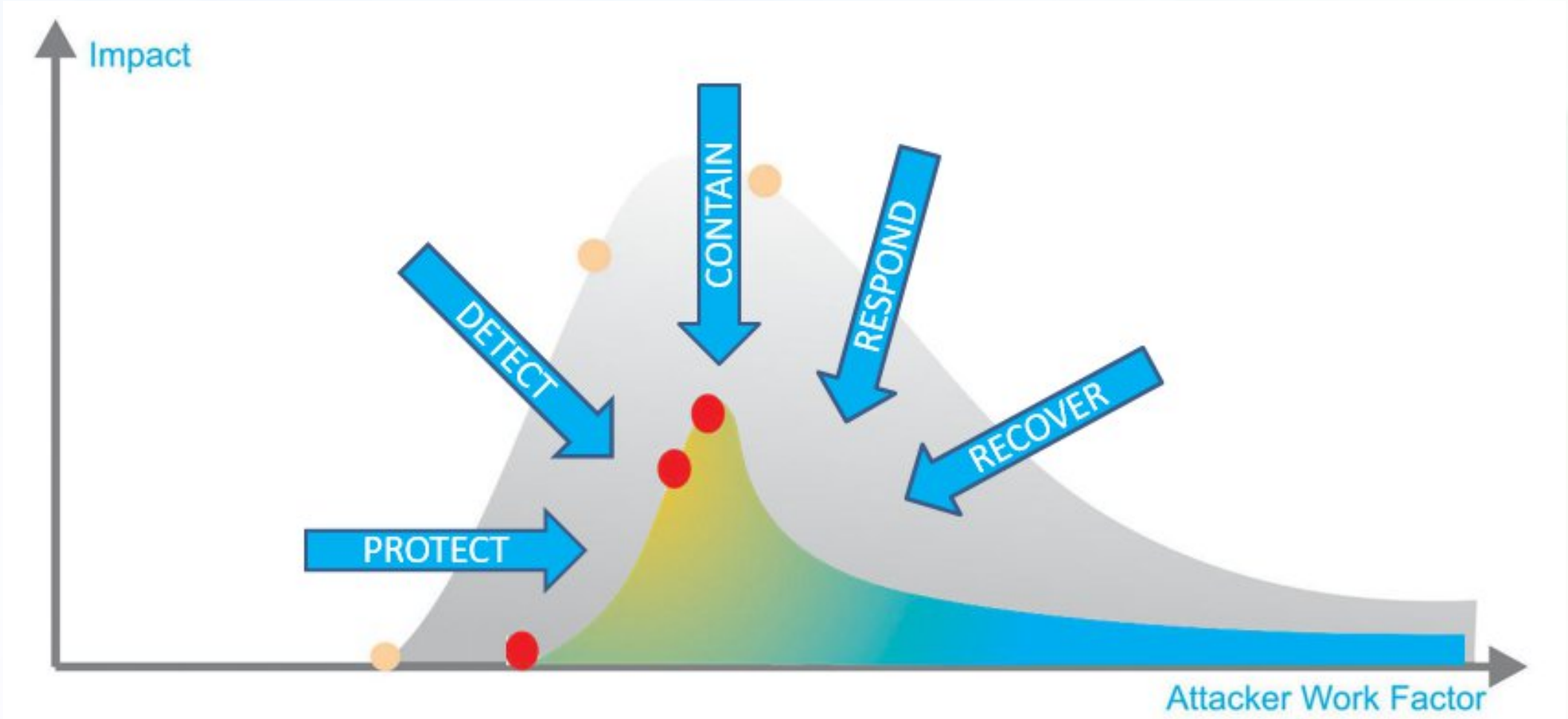
Cyber Security	Cyber Resilience
Protect, Detect and Respond to Cyber Attacks	Anticipate, Withstand, Recover and Adapt to changing Threat landscape
Focus: Defense Against cyber Attacks	Focus: Continuity of Critical functions
Defense Scenario - Detect and Stop the Attack	Assumed Breach Scenarios – Attackers are already inside
Cyber Defense are sufficient	Cyber Defense may Fail
Orientation - Tools & Technology	Orientation – Strategic and Tactical
Cyber Security + Continuity of Operations	Resilience

Building Cyber Resilience

Goals of Cyber Resilience



Objective of Cyber Resilience



Thank You…

E-Mail ID: abhishek.solanki@gov.in

Cloud Security Requirements / Recommendations

- MeitY Empanelled Cloud Service Provider (CSP) with Data Localization Requirements
- Adoption of Regulatory & Security Standards
- Data Protection and Encryption Controls
- Shared Responsibility Model for cloud security
- Right to Audit
- Cloud Risk Assessment and Governance
- Incident Reporting and Response Mechanisms
- Monitoring, Logging, and Periodic Security Audits

DxFS 2026 · ICAI DAAB · Hyderabad · 22-23 May 2026

M V Reddy

SVP & Head – Jio Cloud

Jio Platforms Limited

- Cloud Infrastructure & Platform Engineering
- Cybersecurity & Regulatory Compliance
- Digital Assurance & Continuous Monitoring

Cloud, Cyber Risk & Control

Securing the Digital Enterprise

Regulatory Frameworks Driving Cybersecurity Audits

Industry Perspective – Moving Towards Continuous Assurance

PART 02

Industry Perspective: Moving Towards Continuous Assurance

From annual audit snapshots to always-on, real-time compliance posture

- Continuous Controls Monitoring
- Compliance-as-Code
- AI-Powered GRC
- DevSecOps
- Real-Time Evidence

AI-Led Cyber Attacks: The New Threat Paradigm

AI Threat Landscape

AI has fundamentally shifted the attacker's advantage — speed, scale, and sophistication now outpace traditional defences

10,000+
AI-generated phishing variants/day (2025)

60%
Faster breach execution with AI-automated attacks

$4.88M
Average cost of a data breach (IBM)

3 mins
Time to initial access for AI-assisted intrusion

AI Phishing & Social Engineering

- Generative AI creates hyper-personalised spear-phishing at scale.

Polymorphic & Self-Mutating Malware

- AI-powered malware rewrites its own code to evade signature-based.

Autonomous Lateral Movement

- AI agents autonomously map internal networks, escalate privileges and exfiltrate data without human attacker

How Organisations Are Responding with AI

AI-Powered SIEM: Real-time anomaly detection using behavioural AI

Deception Technology: AI honeypots and decoy assets that detect autonomous reconnaissance bots before they reach real systems

Zero Trust Architecture: AI continuously validates every access request contextually

Threat Intelligence Fusion: AI correlates feeds across global threat databases to predict AI attack vectors 24–48 hours in advance

Industry Signals: The Shift to Continuous Assurance Is Happening

Global standards, India regulation, and enterprise behaviour are all moving in the same direction — simultaneously

80%

of Fortune 500 companies deployed CCM tools by end of 2024

— Gartner

6 mths

FedRAMP 20x: from years to months for cloud compliance authorisation

— GSA USA

35%

reduction in IS audit effort where continuous evidence is deployed

— ISACA

$400B

AI cybersecurity market globally by 2028 (CAGR 23%)

— MarketsandMarkets

Standard / Initiative	What Changed	Impact on Audit Profession
PCI DSS v4.0 (2024)	Mandates continuous control monitoring — annual snapshot no longer sufficient for card payment security	Auditors must evaluate ongoing CCM evidence, not just point-in-time assessments
ISO 27001:2022	Added cloud-specific controls (A.5.23) and explicit requirements for continuous monitoring of information systems	New audit scope covering cloud workload security continuously
CSA CCM v4.0	Cloud controls matrix updated with 197 controls mapped to 22 industry standards simultaneously	Single control framework satisfying multiple regulatory requirements
SEBI CSCRF (India 2024)	Board-level cyber risk mandate + continuous monitoring requirement for all market intermediaries	IS auditors now report directly to board-level governance committees
NIST CSF 2.0 (2024)	Added 'Govern' function — making cyber risk governance a C-suite responsibility, not just IT	Financial auditors must assess governance posture, not just technical controls

Source: Gartner Security & Risk Management 2024 | ISACA State of Cybersecurity 2024 | MarketsandMarkets AI Cybersecurity Report 2025

The Paradigm Shift: Point-in-Time vs. Always-On Assurance

Continuous Assurance

Dimension	TRADITIONAL AUDIT MODEL	CONTINUOUS ASSURANCE MODEL
Audit Frequency	Annual or periodic	Real-time — always on
Evidence Type	Screenshots & documents	Machine-readable, live telemetry
Compliance State	Project-based preparation	Byproduct of daily operations
Audit Readiness	Scramble before audit window	Default state — permanent readiness
Control Validation	Point-in-time testing	Continuous Controls Monitoring (CCM)
GRC Ownership	Separate compliance team	Embedded in DevSecOps pipelines
Risk Visibility	Quarterly/annual reports	Live dashboards & automated alerts

"If your controls fail silently between audit windows, you are non-compliant and vulnerable — whether or not an auditor is watching." — CSA/GRC industry principle

How Continuous Assurance Works in Practice

Technical Architecture

1 Continuous Controls Monitoring (CCM)

- **API-driven evidence collection** replaces screenshots. Live configuration baselines detect drift the moment it occurs.
- **Control failures mapped automatically** to regulatory requirements.
- **Risk scores updated continuously** from threat intelligence feeds.

2 Compliance-as-Code (DevSecOps)

- **Security controls embedded directly in CI/CD pipelines.** Infrastructure-as-Code (IaC) templates carry pre-validated control mappings.
- **Policy-as-code engines** validate every deployment automatically.
- **Misconfigurations caught before production** — not 6 months later.

3 AI-Powered GRC Automation

- **AI-assisted control validation** with plain-language failure explanations for non-technical stakeholders.
- **Automated security questionnaire responses** for regulators and customers.
- **Predictive risk scoring** identifies emerging control gaps before incidents occur.

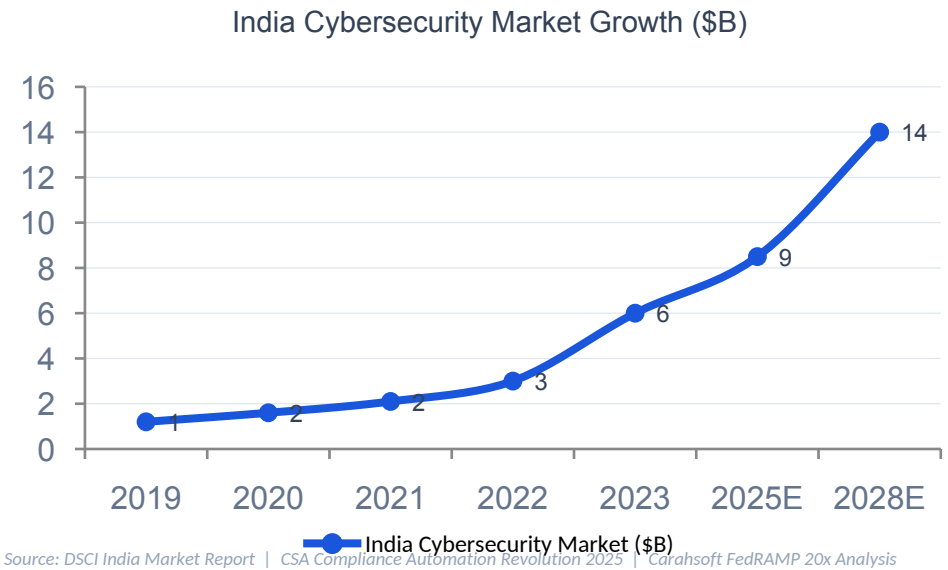
4 Real-Time Compliance Dashboards

- **Leadership sees live regulatory posture** — not quarterly reports.
- **Compliance gaps surface as operational alerts**, not audit findings.
- **Trust centres enable real-time sharing of security posture** with regulators and customers. Audit-ready state becomes the default condition.

The Compliance Automation Revolution

Industry Direction

CSA CAR initiative — from point-in-time certifications to ongoing, real-time confidence in security posture



Source: DSCI India Market Report | CSA Compliance Automation Revolution 2025 | Carahsoft FedRAMP 20x Analysis

Cloud Security Alliance – CAR

Common control libraries, machine-readable regulations and continuous audit processes for regulators to accept real-time evidence.

FedRAMP 20x (Global Benchmark)

27 submissions, 13 authorisations in first pilot. Traditional path: years. Automation: 6 months. RegScale completed SSP in ~3 weeks.

PCI DSS v4.0 Standard

Now demands evidence of continuous control performance — ongoing vulnerability and configuration management, not annual snapshots.

India GRC Skill Gap

Cloud security, DevSecOps and GRC automation are critically under-resourced. Gen AI-powered cybersecurity programs will see a surge in India (DSCI).

What India's Leading Enterprises Are Already Doing

HDFC Bank

Deployed AI-powered SIEM with continuous control monitoring across 100% cloud workloads — audit preparation time reduced by 60%

Infosys

Built compliance-as-code pipeline: every software release auto-validated against ISO 27001, PCI DSS and RBI controls before production deployment

CASE STUDY

HDFC Bank — Building Continuous Cyber Assurance at India's Largest Private Bank

Organisation
HDFC Bank Ltd — India's largest private-sector bank

Scale
94M+ customers · 8,700+ branches · ₹25 lakh crore in assets (FY25)

Regulators
RBI · SEBI · CERT-In · DPDP Act · IT Act 2000

THE PROBLEM

Exponential attack surface: 94M+ digital customers, 8,700 branches, and rapidly expanding API ecosystem

Perimeter-based defences inadequate against AI-driven lateral movement and polymorphic malware

Alert fatigue: traditional SIEM generating thousands of low-context alerts daily

Manual compliance workflows creating audit blindspots

Board demanding real-time cyber risk visibility— **no live dashboard available**

WHAT THEY BUILT

Next-Gen SOC: Purpose-built for predictive incident management

AI/ML-enabled SIEM fed by 10,000+ logging sources— unified real-time threat visibility

SOAR deployed to automate incident triage, containment and response

Network micro-segmentation across critical banking infrastructure

Agentic AI security bots — autonomous agents handling Tier-1 SOC tasks.

VALUE REALISED

10,000+	Logging sources feeding AI/ML SIEM
Near-Zero	External internet-facing application vulnerabilities sustained
Predictive	SOC operating in predictive mode
Automated	Incident response via SOAR
AI-First	Board-mandated AI-first security roadmap underway with Agentic bots

> ***"The journey toward effective cyber resilience starts with simplifying complexity — automation is no longer optional, it's inevitable."***
> *— Sameer Ratolikar, Group Head & CISO, HDFC Bank (BankInfoSecurity, May 2025)*

Source: HDFC Bank Integrated Annual Report FY22 (Digitisation chapter) | Finacle Banking Trends Report 2026 | BankInfoSecurity — AI Bots Take Over Cybersecurity at HDFC Bank, May 2025

JioCloud:
Engineering Compliance into Sovereign Cloud

JioCloud in Practice

India's largest cloud platform — built for regulatory-aligned, sovereign digital infrastructure for regulated enterprises

1 Security Built Into the Platform Layer

Security logging, access governance, network segmentation and encryption are platform primitives — not optional add-ons

Every workload inherits a security baseline that is audit-ready by default

OpenStack + Ceph: 100PB+ capacity across 5+ seismic zones in India

CERT-In-aligned incident detection and 6-hour reporting infrastructure

2 Shared Responsibility Done Right

Crystal-clear, documented control handoffs — JioCloud vs. customer responsibilities

Control mapping documentation aligned to CERT-In, DPDP, RBI and SEBI frameworks

Enterprise customers use JioCloud shared evidence for their own regulatory submissions

ISO 27001 and SOC 2 certification postures reducing customer audit overhead

3 Real-Time Compliance Visibility

Integrated CSPM (Cloud Security Posture Management) and continuous vulnerability assessment

Data residency guarantees for DPDP localisation and sector-specific requirements

Compliance gaps surfaced as operational alerts — not audit findings after the fact

JioCloud roadmap: live regulatory compliance dashboard for enterprise customers

JioCloud + Microsoft Azure: World-class reliability, performance and compliance for BFSI, government and regulated industry — on Indian infrastructure.

Challenges on the Road to Continuous Assurance

Skills Gap

- Cloud security, DevSecOps and GRC automation are severely under-resourced in India.
- Demand for CERT-In empanelled auditors will rapidly outstrip supply.

Board-Level Literacy

- Continuous assurance generates enormous security telemetry.
- Leadership must consume risk dashboards and make capital decisions from real-time posture data

Supply Chain & Third-Party Risk

- CERT-In 2025 explicitly requires SBOM/HBOM/AI-BOM and vendor risk accountability.
- Continuous assurance must extend beyond the enterprise perimeter.

Regulatory Fragmentation

- CERT-In + DPDP + RBI + SEBI + Telecom = parallel compliance streams with no bridging guidance.
- Industry needs a single control set satisfying multiple regulators.

Regulator Readiness

- Continuous assurance delivers full value only when regulators accept machine-readable, continuous evidence submissions.

Investment Justification

- GRC automation must be framed in business terms: accelerates deal cycles, reduces breach risk, lowers manual overhead.

The Road Ahead: AI-Driven GRC & India's Opportunity

Future Outlook

India's Sovereign Assurance Opportunity

- DPDP + CERT-In + sector rules = massive demand for continuous assurance infrastructure
- Indian cloud providers deliver sovereign, regulatory-aligned CCM that global platforms cannot replicate with domestic regulatory intelligence
- JioCloud positioned as compliance infrastructure — not just compute — for India's regulated enterprises
- 5% of global cybersecurity market by 2028 expected from India (DSCI projection)
- Gen AI-powered cybersecurity programs, data privacy & cyber resilience investments surging
- CAs mastering continuous assurance methodology become the trusted cyber assurance providers of the next decade

AI + GRC: What's Coming Next

Agentic Compliance
AI agents autonomously collect evidence, test controls and generate audit artefacts without human prompting

AI-Powered Audit Scoring
CSA Valid-AI-ted: AI scoring rubric for cloud provider compliance

Machine-Readable Regulations
Regulatory NLP enables AI to auto-map new laws to existing control frameworks

Predictive Risk Intelligence
AI predicts control failures using telemetry patterns before incidents

AI Governance Regulation
DPDP Act expected to expand into AI Governance

Source: SISA Infosec Cybersecurity Outlook | CSA Compliance Automation Revolution | DSCI India Market Projections | EY DPDP Rules 2025

Key Takeaways

Regulation is Moving Fast

- CERT-In 2025, DPDP Act, RBI, SEBI CSCRF and Telecom Rules represent a structural shift — not incremental change.
- The compliance gap is a board-level financial risk today.

AI Has Changed the Threat

- AI-powered attacks — polymorphic malware, deepfake fraud, autonomous lateral movement — outpace traditional defences.
- Security must now fight AI with AI.

Continuous Assurance is Available Now

- The technology exists — CCM, compliance-as-code, AI-powered GRC.
- Early movers gain competitive advantage in trust, deal cycles, and regulatory relationships.

Cloud Providers are Compliance Infrastructure

- Sovereign, regulatory-aligned cloud is the foundation of India's digital enterprise security.
- Security must be engineered in, not layered on. JioCloud is built on this principle.

IS Auditors Must Lead the Transition

- The professionals in this room are at the intersection of governance, regulatory compliance and digital assurance.
- The IS Auditor of 2030 is a Continuous Assurance Practitioner.

India's Sovereign Opportunity

- 5% of the global cybersecurity market by 2028. Sovereign cloud + regulatory alignment + CA expertise = a uniquely Indian competitive advantage in digital trust.

Thank You

"The digital enterprise is only as secure as the platform beneath it, the regulatory clarity above it, and the governance culture within it."

M V Reddy

Senior Vice President & Head – JioCloud, Jio Platforms Limited

DxFS 2026 · Digital Transformation Finance Summit · ICAI DAAB · 22–23 May 2026 · Novotel Hyderabad Convention Centre

FROM CLOUD ADOPTION
TO CYBER RESILIENCE

A Strategic Journey to Securing the Digital Enterprise

Dr. Saurabh Maheshwari | DxFS 2026 Hyderabad

The Invisible Backbone

~100% CLOUD DEPENDENCY

Powering Daily Life: Almost every digital interaction routes through remote data centers.

Photos, contacts, and device backups sync seamlessly via platforms like Google Drive, iCloud, and Dropbox.

Smart home devices and streaming platforms (Netflix, Spotify) pull content directly.

Real-time location and traffic data power commutes and ride-sharing (Uber, Ola).

Enabling Mobile Front-Ends: Local devices simply pull remote data.

Food delivery, social media, and fitness apps store user data, process complex orders, and trigger notifications entirely via the cloud.

Developers bypass constant app store downloads, pushing features, bug fixes, and security patches seamlessly behind the scenes.

94% of Enterprises rely on cloud services, replacing physical on-premises servers.

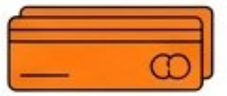
Total reliance on software like Microsoft 365, Salesforce, and Slack for collaboration.

The gig economy and retail spikes depend on elastic power to scale up during holiday sales without crashing.

Training and deploying generative AI requires the massive horsepower of hyperscale cloud platforms.

99% Uptime enabled by modern cloud architectures.

Legacy systems replaced. 24/7 access to checking accounts and transaction viewing.



Digital payment rails and point-of-sale (POS) systems demand instant, cloud-based transaction routing.

Machine learning algorithms run continuously in the cloud to detect unusual spending and halt fraudulent activity instantly.

Source Data tracked via Prioxis Cloud Computing Statistics & IBM Cloud Adoption Overview

Cloud is No Longer an IT Choice. It is the New Business Operating Model.

The shift from a technology decision to a fundamental business architecture decision.

For modern enterprises, cloud is not merely “where the client’s data is stored.” It is the digital foundation on which business transactions, financial controls, compliance processes, audit evidence, and stakeholder trust now operate.

State of Cloud Security 2026: The Expanding Perimeter

200 ZB

Total data stored in the cloud by 2026

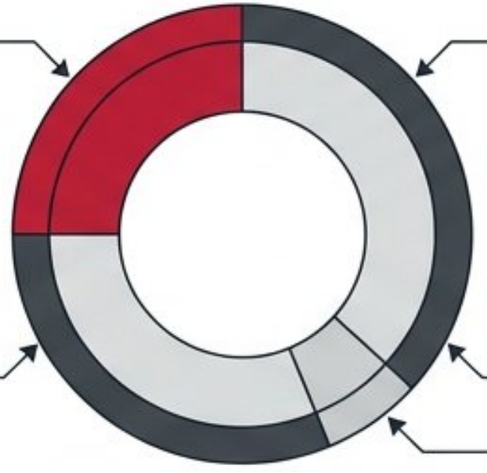
45%

Proportion of all global data breaches occurring in the cloud

154%

Year-over-year surge in significant cloud breaches

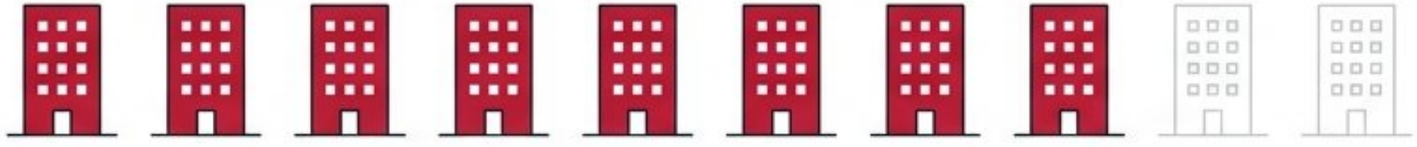
Global Average Breach Cost: $5.17M



US Average Breach Cost: $10.22M
(Driven by regulatory fines and detection expenses)

Detection Gap: 277 Days
(Average time to identify/contain a multi-cloud breach)

Operational Halt: 24 Days
(Average downtime after a cloud ransomware attack)



80% of organizations experienced at least one cloud security breach in the past year, making incidents a routine operational reality rather than an exception.

The Twin Pillars of Risk: Diagnosing the 2026 Attack Surface

Human Error & Misconfiguration

95% Cloud security failures stemming from misconfigurations (manual errors).

88% Total data breaches driven by human error.

73% Organizations affected by phishing (the most prevalent cloud breach vector).

32% Cloud infrastructure sitting idle and unmonitored (averaging 115 vulnerabilities each).

The Automation Threat: Attackers now use AI to launch large-scale exploits faster than human teams can patch.

Identity & System Exploits

>70% Cloud breaches originating from compromised identities.

68% Organizations citing account takeovers as their leading security concern.

91% Organizations harboring security flaws older than 10 years (46% over 20 years old).

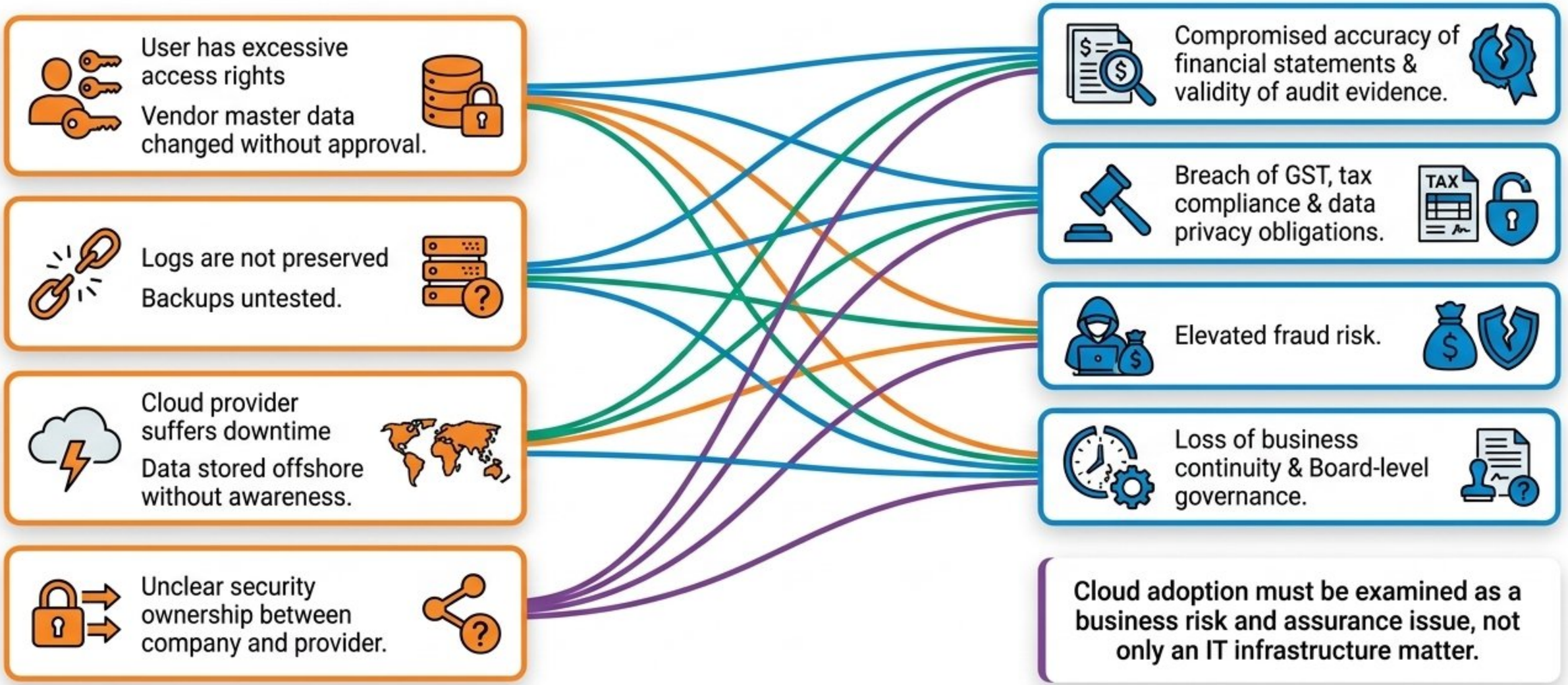
Key Insight: Non-human identities (service accounts, API keys) are exploding, creating new vulnerabilities for automated bots.

The Enterprise Cloud Ecosystem

Technology is no longer a background support function; it is the engine driving every business area.

The Risk Domino Effect

Scenario: Mid-Sized Manufacturing Company running purchase orders, inventory, and GST on a Cloud ERP.



The Evolution of the Professional Mandate

The Past

ROLE:
Financial Statement Professional

PRIMARY QUESTION:
"Is my client using cloud?"

MINDSET:
Technology as a distant background support function.

The Present & Future

ROLE:
Digital Trust Professional

PRIMARY QUESTION:
"How deeply is my client's financial and operational trust dependent on cloud?"

MINDSET:
Technology as the source of business risks that must be governed, controlled, and monitored.

When business runs on cloud, assurance cannot remain on paper.

Cyber Risk Has Moved from Server Rooms to Boardrooms

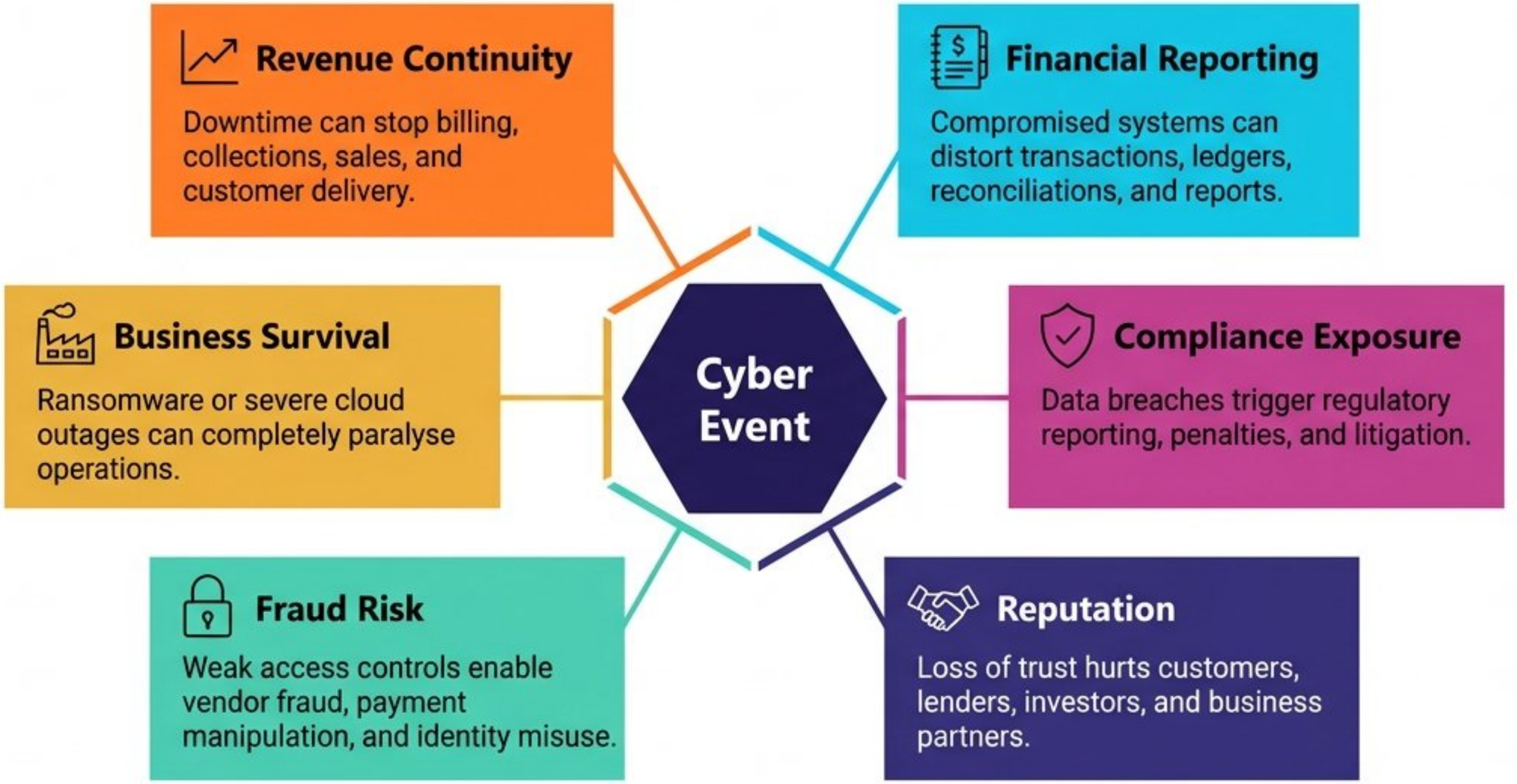
The Old Question:
Are our systems secure?

Limited to firewalls, passwords, antivirus, and network security.

The New Question:
Can our business continue, comply, report, recover, and retain trust?

Cyber risk is no longer a separate technical issue. It is a business, financial, compliance, operational, and governance risk wrapped inside a digital system.

The Business Impact Framework



When an incident happens, the damage travels straight from the IT department into the boardroom.

Cloud Gives Speed. Resilience Builds Trust.

"Cloud adoption without cyber resilience is digital acceleration without brakes, seatbelts, or emergency exits."

How fast can we go digital?

- Speed
- Flexibility
- Scale
- Capital Reduction

How safely can we continue when disrupted?

- Continuity
- Recovery
- Response
- Evidence

Trust is not created by adoption alone. Trust is created by control, evidence, discipline, review, governance, and accountability.

From Adoption to Assured Resilience

Cloud Adoption Gives...

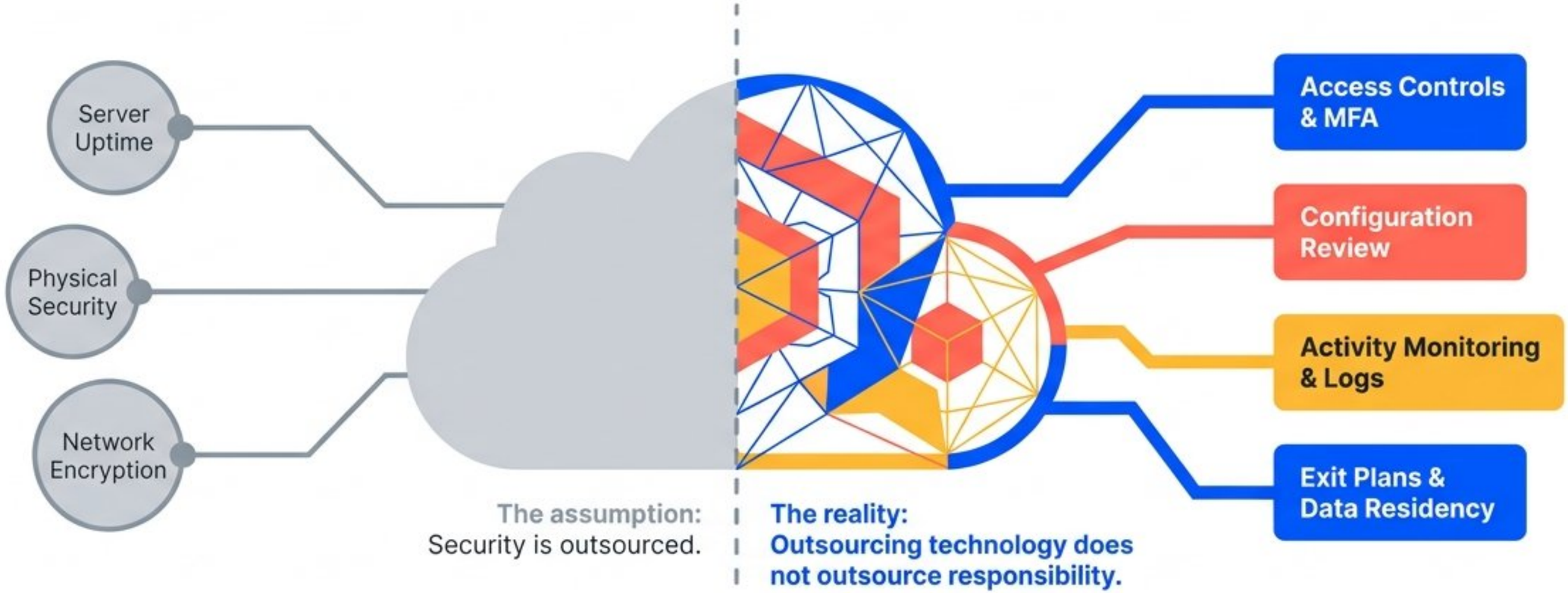
- Faster deployment
- Remote accessibility
- Cost flexibility
- Scalable infrastructure
- Digital workflows
- Business automation
- Data availability

Cyber Resilience Ensures...

- Safe and controlled deployment
- Secure and monitored access
- Risk-aware cost optimisation
- Tested recovery capability
- Reliable audit trails
- Continuity during disruption
- Data integrity and protection

For the Chartered Accountant, the real assurance question is not “Has the organisation adopted cloud?” but “Can the organisation remain trusted, compliant, and operational when its cloud-dependent business faces disruption?”

Cloud Risk is Rarely a Cloud Failure.
It is a Governance Failure.



Is the organisation in control of its cloud environment, or is it merely using cloud without governing it?

The Three Hidden Vectors of Cloud Risk

Misconfiguration Risk

Cloud environment is not set up securely.

Technical Faults: Open network ports, missing MFA, unrestricted admin privileges.

Business Impact: Exposure of GST records, payroll files, patient info; severe legal liability.

The Audit Question: Have cloud security settings been formally reviewed, approved, and periodically tested?

Weak Governance Risk

Cloud sprawl outpacing central oversight.

Technical Faults: Departments buying disjointed SaaS tools, duplicate systems, no exit plan.

Business Impact: Loss of data visibility, fractured accountability, incomplete assurance records.

The Audit Question: Who owns each platform, and what data is shared with them?

Third-Party Exposure

High dependency on external vendors (SaaS, API, gateways).

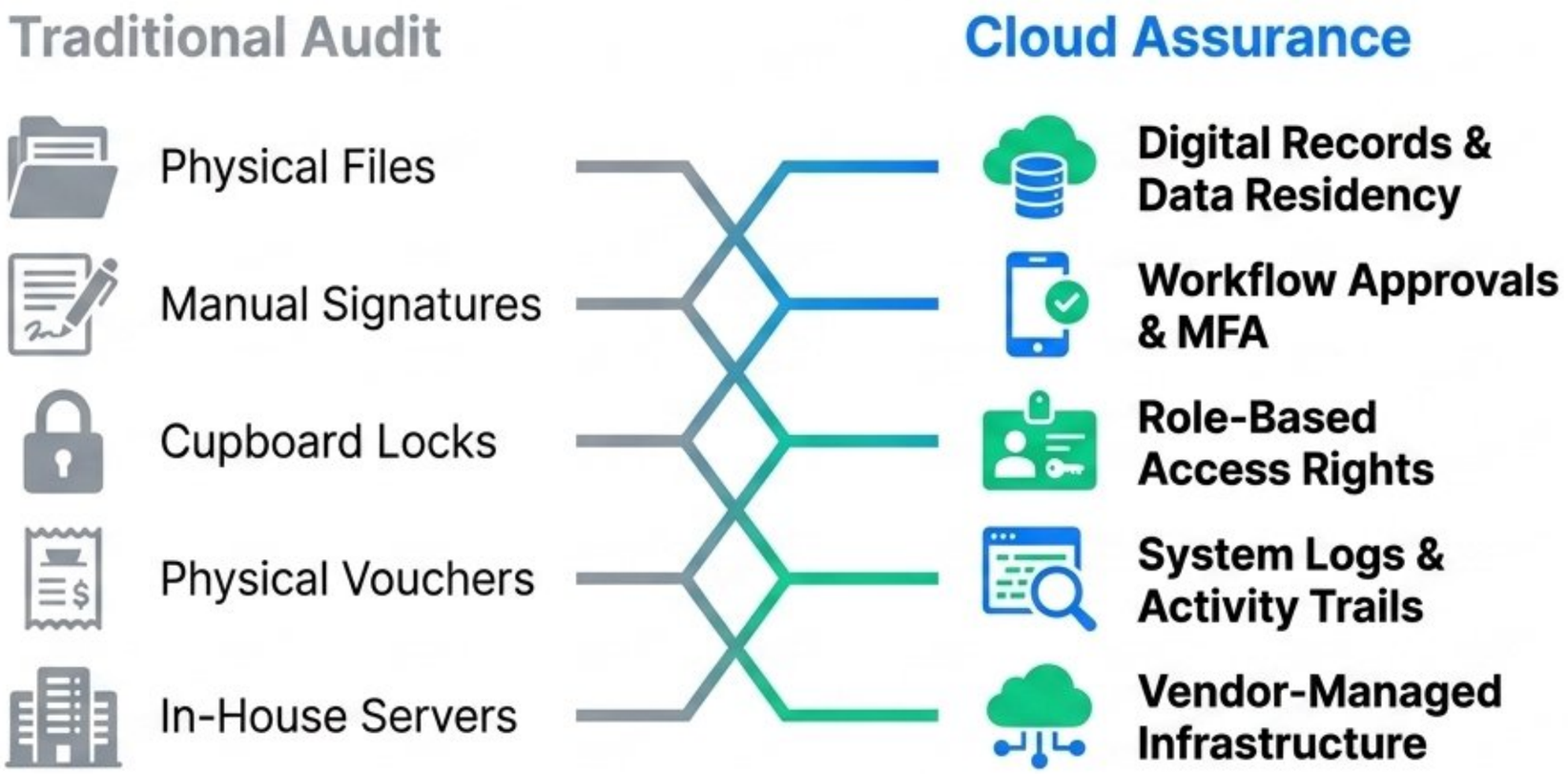
Technical Faults: Vendor failure, lack of breach reporting contracts.

Business Impact: Total business disruption, compliance breaches, data hostage situations.

The Audit Question: If the vendor fails, is the business still accountable? (Answer: Yes.)

Only the Environment Has Changed. The Audit Mindset Remains.

The CA does not need to become a cloud engineer. They must simply ensure the environment is governed, controlled, monitored, and auditable. We still ask: Who has authority? What evidence exists? Is there segregation of duties?



A company may appear digitally mature, but internally it may be digitally scattered.

The CA brings structure, accountability, and visibility.

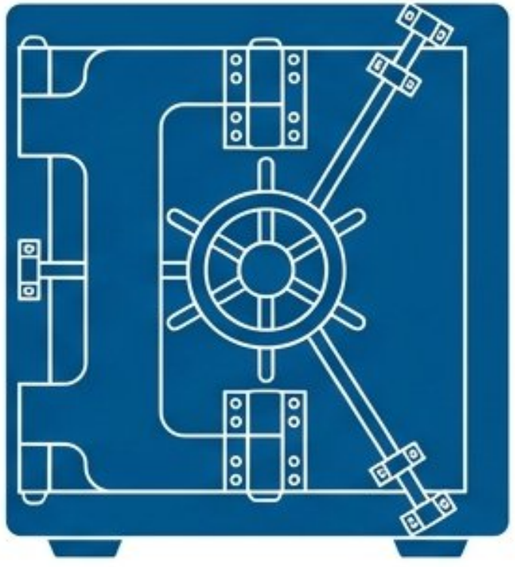
The 10-Point Cloud Governance Diagnostic

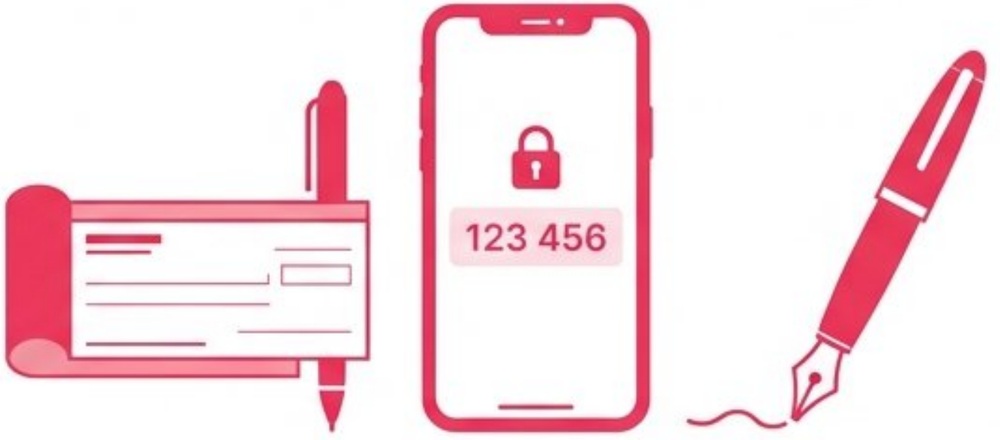
*Diagnostic in Action: A healthcare client uses cloud software for billing, prescriptions, and HR. During a review, a CA finds shared logins, former employees with access, untested backups, and unknown third-party analytics data storage. This is not software risk; this is **compliance, privacy, and board governance risk.***

Cloud risk begins where governance ends.

In Cloud, Security is Shared, but Accountability is Not

~~We are safe because we use a reputed cloud platform.~~





The Provider

Analogy: The bank secures the physical vault.
Cloud Reality: The cloud provider secures the core cloud infrastructure.

The Organisation

Analogy: You secure your passwords, OTPs, and transaction approvals.
Cloud Reality: The organisation must secure its use of the cloud.

Outsourcing the platform does not outsource management responsibility.
This misunderstanding creates a dangerous gap between perceived security and actual assurance.

Drawing the Security Boundary

Provider Capability (The Foundation)

- Physical data centre security
- Core cloud infrastructure
- Platform availability (SLA uptime)
- Providing logging, encryption, and toolsets

Customer Control (The Execution)

- Identity, passwords, and user access
- Data protection and classification
- Business application controls
- Enabling, reviewing, and preserving logs
- Assessing compliance evidence
- Responding to business-side incident impacts

A reputed provider does not automatically protect an organisation from weak passwords, excessive admin rights, unapproved vendor changes, or a lack of log review.

Continuous Business Requires Continuous Assurance

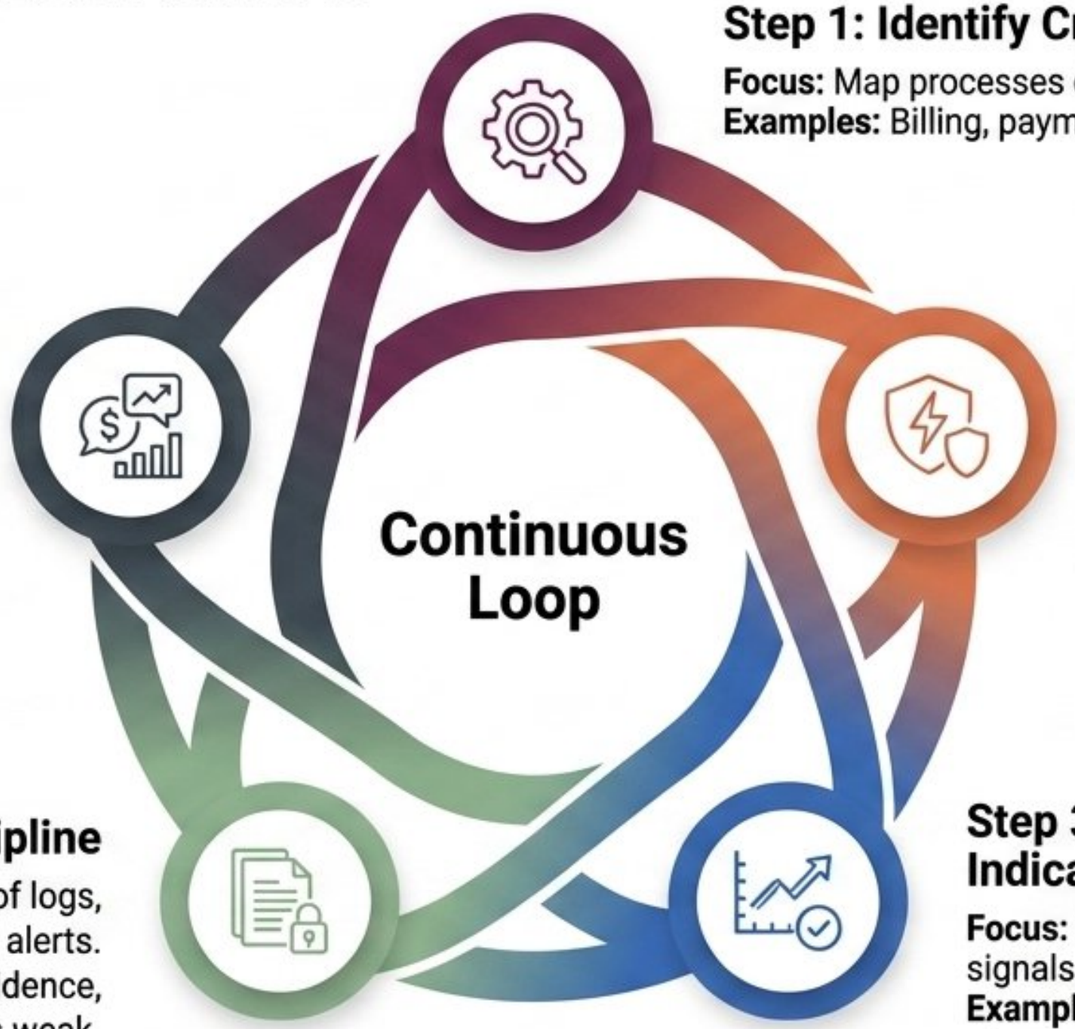
Traditional Control Thinking	Continuous Assurance Thinking
Periodic checking	Ongoing monitoring
Sample-based review	Data-driven review
Manual evidence collection	System-generated evidence
Static control checklist	Dynamic control dashboard
Post-event detection	Early warning indicators
Siloed audit approach	Integrated business, cyber, and compliance view

Evolution Bridge

From: Were controls present at the time of audit?

To: Are critical controls continuously working, monitored, and evidenced?

The Five-Step Framework for Continuous Assurance



Step 1: Identify Critical Digital Processes

Focus: Map processes dependent on cloud systems.
Examples: Billing, payments, statutory filings, financial closing.

Step 2: Identify Key Digital Risks

Focus: Understand what can go wrong in real-time.
Examples: Data leakage, wrong configuration, vendor failure.

Step 3: Define Key Control Indicators

Focus: Create measurable, continuous signals.
Examples: Failed logins, vendor master changes, backup failures.

Step 4: Build Evidence Discipline

Focus: Automate the retention of logs, approvals, and alerts.
Rule: Without system-generated evidence, assurance is weak.

Step 5: Report Exceptions in Business Language

Focus: Translate technical alerts into board-level impacts.
Action: Moving from "Three privileged accounts active" to "Three users can alter financial records."

The Expanded Role of the Cloud-Era Auditor

The future of assurance is not only periodic verification.
It is continuous visibility into critical risk.

What Should a CA Audit in a Cloud-Enabled Business?

The Myth: Auditing Servers

A purely technical domain of complex diagrams and security dashboards

The Reality: Auditing Trust

A business, control, compliance, and assurance environment.

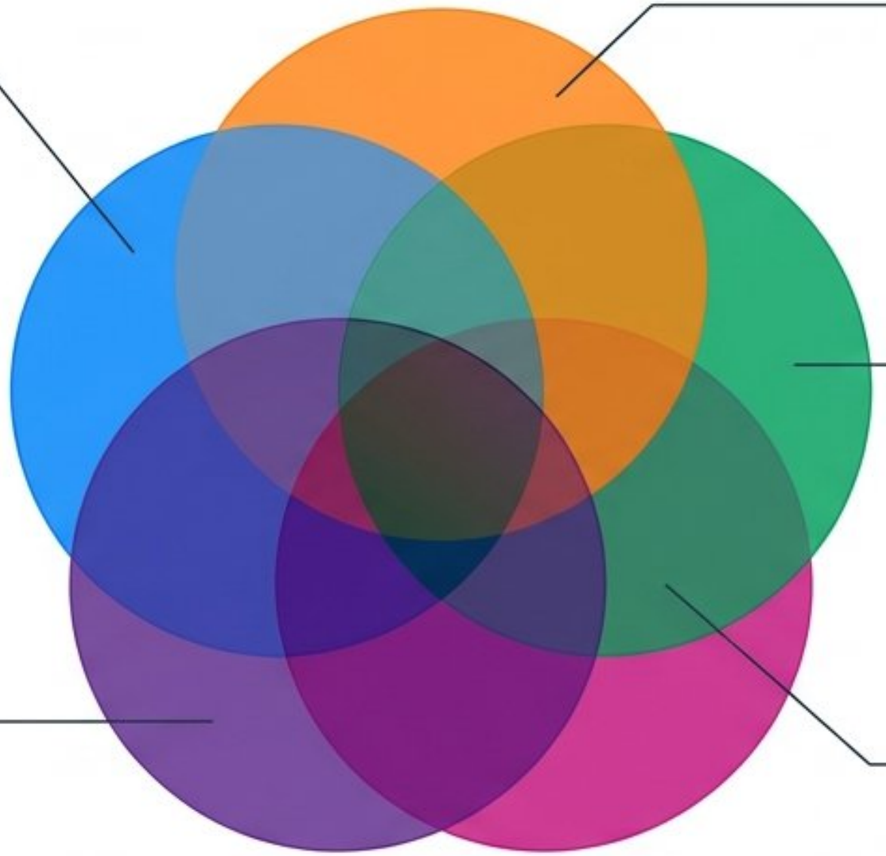
Which business processes are running on cloud, and what can go wrong if those systems are misused, unavailable, compromised, or unreliable?

Cloud audit is not only about the cloud provider. It is about the client's governance over cloud usage.

The 5 Lenses of Cloud Assurance

Governance

Who owns cloud risk? Focuses on cloud usage policies, application approvals, and eliminating Shadow IT.



Control

Are business controls working? Automation does not equal control. Focuses on maker-checker setups and access reviews.

Compliance

Are legal requirements mapped? Cloud does not reduce compliance. Focuses on RBI, SEBI, DPDP Act, and GST record retention.

Evidence

Can generated evidence be trusted? The spine of assurance. Focuses on log integrity, timestamps, and report alteration.

Continuity

Can the business continue? Vendor uptime does not equal business readiness. Focuses on ransomware, SaaS failures, and tested recovery.

The 5 Pillars of India's Digital Compliance Landscape

Decoding the specific cyber and data expectations across key sectors.

RBI

Technology & Financial Governance

Focus

IT governance, risk, controls, BCP/DR, third-party dependency.

The CA Perspective:
Technology is not merely an operational matter. It Is a governance and assurance matter.

SEBI

Market Trust & Cyber Resilience

Focus

Withstand/recover capability, access controls, vulnerability management.

The CA Perspective:
Resilience means the ability to operate, respond, recover, and preserve market trust.

IRDAI

Policyholder Trust & Data Privacy

Focus

Information security governance, lifecycle controls, KYC/health data.

The CA Perspective:
In insurance, cyber risk is not only system risk. It is policyholder trust risk.

CERT-In

Incident Discipline & Evidence

Focus

Mandatory 6-hour reporting, log retention, time synchronisation.

The CA Perspective:
You cannot report an incident in six hours if it takes six days to discover who owns the system.

DPDP Act

Data Protection & Accountability

Focus

Lawful processing, principal rights, safeguards, breach notification.

The CA Perspective:
Data protection is a control system that must operate inside the business, not merely a privacy policy on a website.

Not Just Protection, But Preparedness and Recovery

Cybersecurity

Focuses on protecting systems, networks, and data from attacks.

The Flawed Question: Can we prevent every attack?

Cyber Resilience

Preserves business continuity, financial integrity, regulatory compliance, and stakeholder confidence.

The Mature Question: If something goes wrong, can we detect, respond, recover, and continue with minimum damage?

The Cyber Resilience Lifecycle

Learn

Convert the incident into institutional improvement.

CA Assurance Focus: Track root cause analysis, lessons learned, and audit committee/board reporting.

Prepare

Build readiness before the incident.

CA Assurance Focus: Verify policies, enterprise risk register, BCP, cyber insurance, and clearly defined roles.

Recover

Restore business safely and reliably.

CA Assurance Focus: RTO (tolerate downtime?), RPO (acceptable data loss limits?), Backup (successfully tested for restoration?).

Detect

Know early that something has gone wrong.

CA Assurance Focus: Ensure logs are enabled, alerts are monitored, and exception reports are generated.

Respond

Act quickly to contain damage.

CA Assurance Focus: Validate incident response plans, decision/escalation matrices, and strict evidence preservation.

The CA's Unique Advantage: The Translation Engine

We do not replace the technologist; we convert technical risk into business consequence.

Technical professionals can **configure** systems. CAs bring **accountability, governance and**

The Six Pillars of Digital Trust Assurance

A comprehensive ecosystem of new professional practice areas for the digital economy.

Cloud Assurance

Review cloud governance, access controls, backup policies, and application audit trails.

Cyber Risk Advisory

Translate cyber vulnerabilities into business, financial, operational, and compliance risk registers.

Digital Trust Audit

Assess whether ERP reports, digital logs, approvals, and AI outputs are reliable for audit evidence.

Regulatory Compliance

Convert RBI, SEBI, CERT-In, and DPDP regulations into practical, auditable operating controls.

Third-Party & SaaS Risk

Review SaaS vendor due diligence, data ownership, SLAs, breach reporting, and exit clauses.

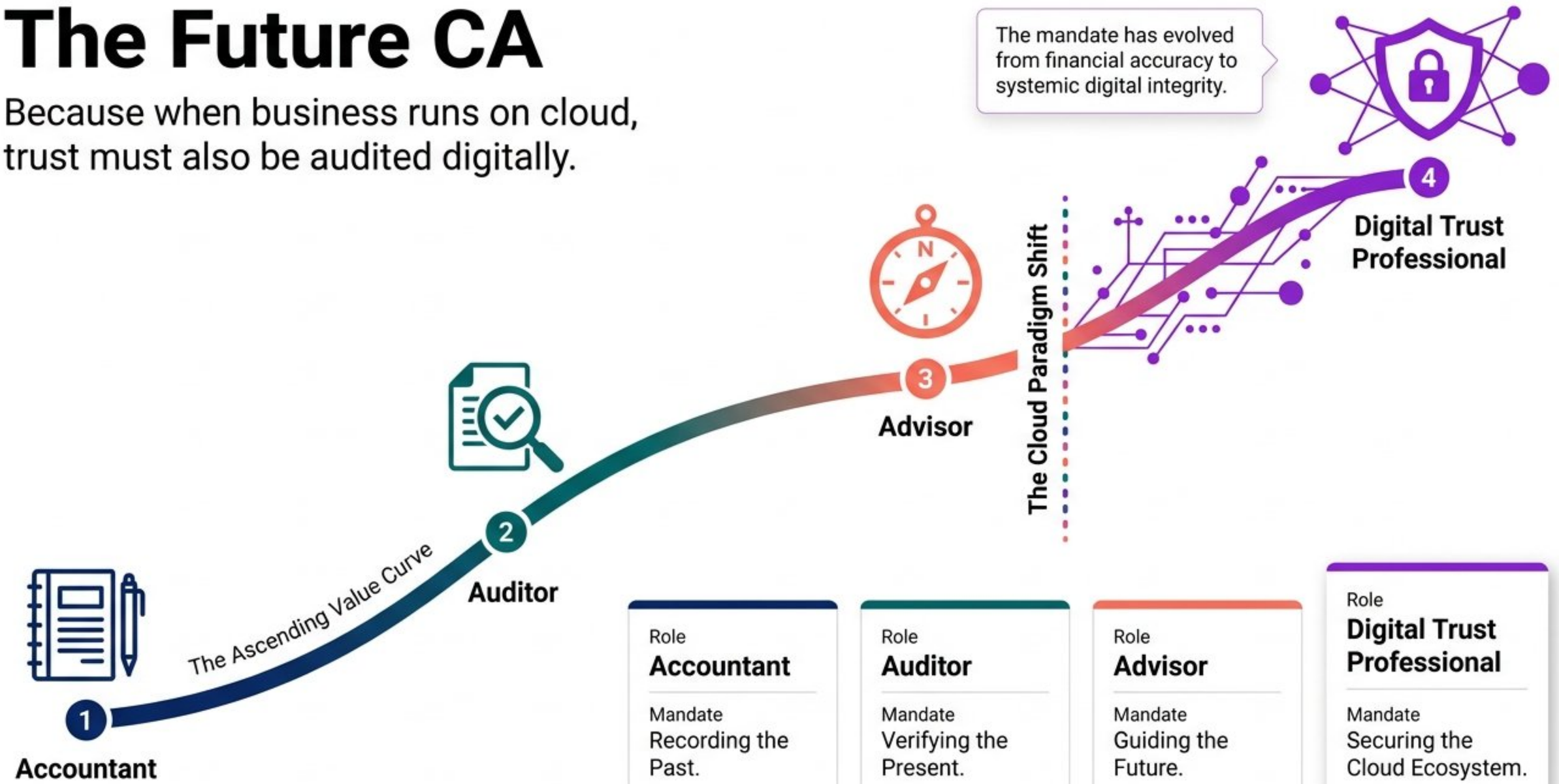
Business Resilience

Assess Disaster Recovery, Business Continuity Plans, and evidence of ransomware readiness.

The Future CA

Because when business runs on cloud, trust must also be audited digitally.

The mandate has evolved from financial accuracy to systemic digital integrity.

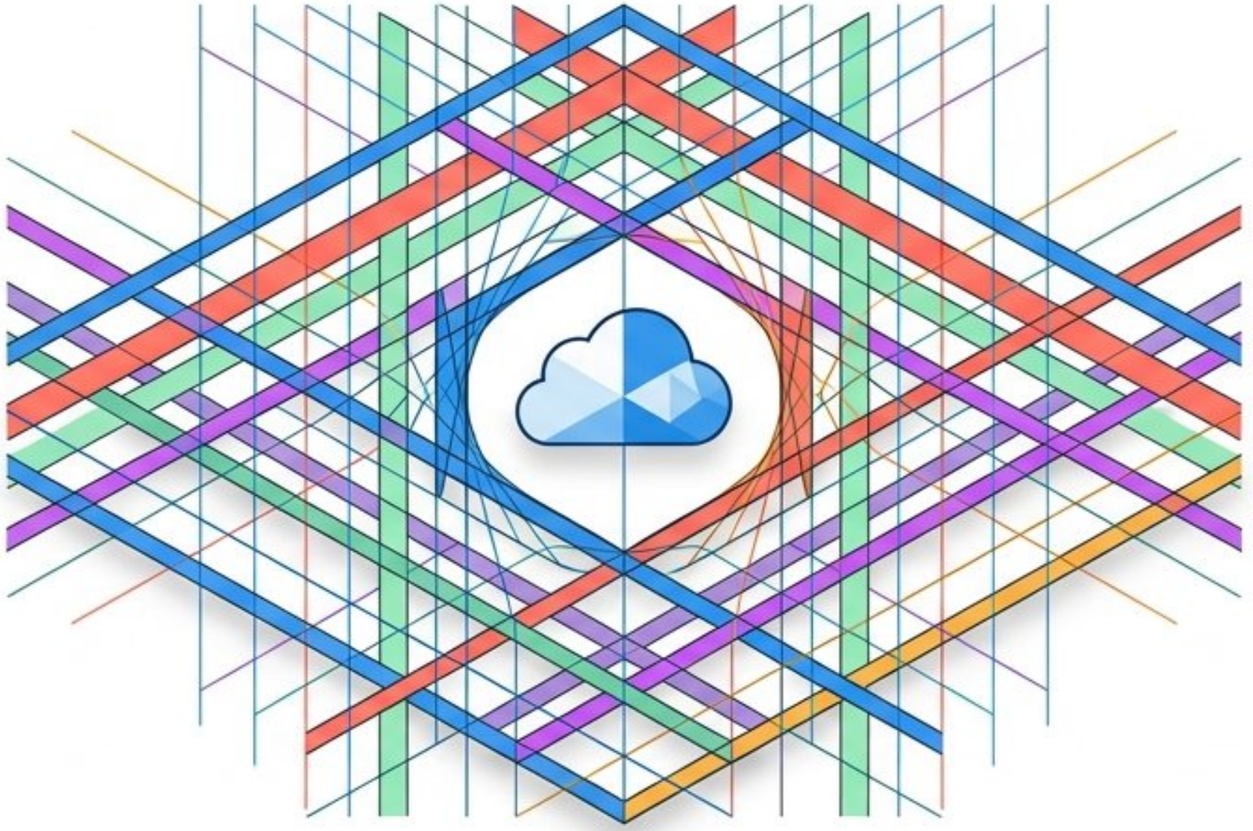


Role	Role	Role	Role
Accountant	**Auditor**	**Advisor**	**Digital Trust Professional**
Mandate Recording the Past.	Mandate Verifying the Present.	Mandate Guiding the Future.	Mandate Securing the Cloud Ecosystem.

Saurabh Maheshwari

Technology Simplified

+91 98292 03200 | saurabh@sklztect.com



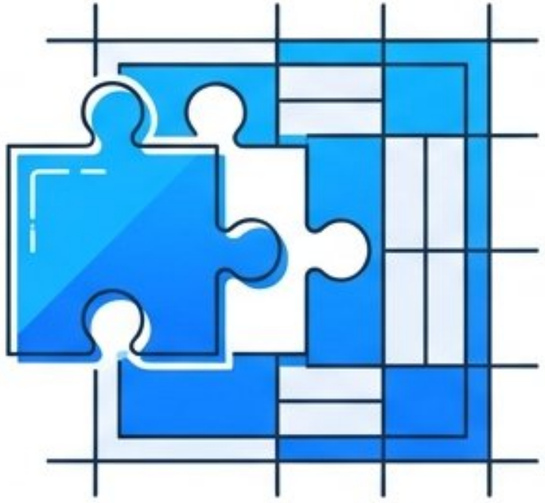
The Chartered Accountant’s Cloud Playbook

21 Critical Diagnostic Parameters for Evaluating Cloud Service Providers.

For modern auditors, the cloud is no longer just an IT line item—it is the foundation of business continuity. This playbook transitions the CA’s role from simply validating technology expenditures to rigorously interrogating third-party operational dependencies.

Aligning Cloud Adoption with Business Reality and Financial Truth

Point 1: Business Fitment



Before evaluating the provider, the CA must understand why the client wants the cloud.

CA's Core Question:
Is the CSP suitable for the client's actual business need, or is the client simply buying technology without a clear business case?

- ✓ Business Case
- Technology Hype

Point 2: Financial Viability & TCO

For MSMEs, cloud looks cheaper at first, but hidden costs quietly multiply over time.

CA's Core Question:
Is the cloud solution truly economical over the lifecycle, or only attractive on day one?

- ✓ Economical (3-5 Years)
- ✗ Cheap First Invoice

Evaluating Partner Reliability and Protecting Data Sovereignty

Point 3: CSP Reputation & Stability

The CSP must be evaluated as a serious, critical third-party dependency.

CA's Core Question:
Can the client genuinely rely on this CSP as an enduring business partner, not just a software vendor?

✓ Long-Term Partner

Software Vendor

Point 4: Data Ownership & Portability

This is one of the most vital review areas for a CA.

CA's Core Question:
Can the client unconditionally access, control, retrieve, retain, and delete its own data when required?

✓ Complete Control

✗ Hostage Data

Validating Defensive Posture and Ensuring Audit Trail Availability

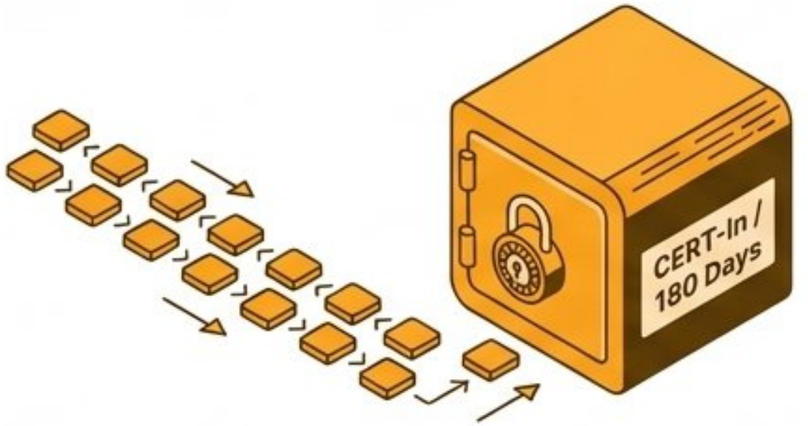
Point 5: Information Security Controls

CAs need not perform deep technical testing, but must verify that **essential, evidenced controls** exist.

CA's Core Question:
Does the CSP provide controls tailored and adequate for the **specific criticality** of the client's data?

Adequate for Sensitivity ✓ | ✗ Generic Protection

Point 6: Logging & Monitoring



CERT-In's 2022 directions require specified cyber incidents to be reported in six hours, and ICT logs maintained for 180 days in India.

CA's Core Question:
If something goes wrong, will the organization have **reliable evidence** to investigate, report, and prove what happened?

Reliable Evidence ✓ | ✗ Operational Blindness

Navigating the Complexities of Privacy Law and Sectoral Regulations

Point 7: Privacy & DPDP Readiness

The Digital Personal Data Protection Act establishes the **individual's right** to protect data and mandates lawful processing.

CA's Core Question:

Will the CSP help demonstrate **responsible data handling**, or create **hidden privacy exposure** under the Act?

Responsible Handling ✓ ✗ Hidden Exposure

Point 8: Regulatory & Sectoral Compliance

For **regulated** entities, evaluation must align with sectoral expectations (e.g., RBI's strict IT **governance** and **IS audit** directions).

CA's Core Question:

Does the arrangement actively help the client comply with applicable laws, or does it introduce **regulatory ambiguity**?

Regulatory Alignment ✓ ✗ Compliance Uncertainty

Securing Enforceable Continuity Promises and True Disaster Recovery

Point 9: SLA & Performance Commitments

The SLA is not a decorative document; it is the fundamental operating contract of business continuity.

CA's Core Question:
Does the SLA tangibly protect business continuity, or does it merely offer comforting best effort support?

Guaranteed Continuity ✓ | ✗ Best-Effort Promises

Point 10: Backup, DR & Business Continuity

The cloud platform may remain highly available, but the client's internal business operations may still be vastly unprepared.

CA's Core Question:
Can the client actually recover operations during a disaster, or is backup merely a reassuring buzzword in the proposal?

Actual Recovery Capability ✓ | ✗ Comforting Proposal Words

Managing Active Incidents and Unmasking Invisible Supply Chains

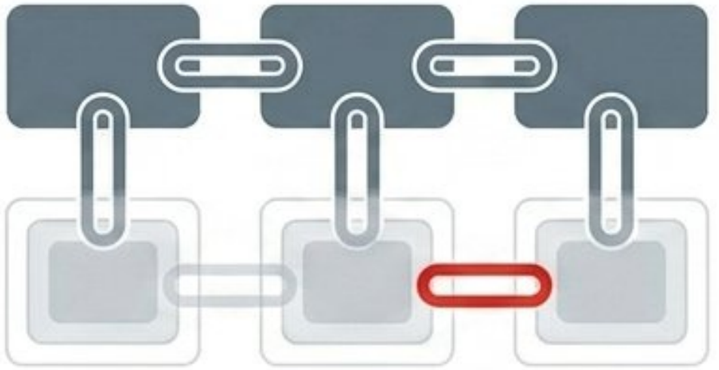
Point 11: Incident Response & Breach Management

A CSP must be evaluated not just for how it prevents breaches, but how it behaves during an active crisis.

CA's Core Question:
When an incident inevitably happens, will the CSP become an active support partner or a defensive silence machine?

Support Partner ✓ ✗ Silence Machine

Point 12: Supply Chain & Sub-Processor Risk



The CSP likely depends on other providers. The client is obligated to map this cascading risk.

CA's Core Question:
Is the client intentionally trusting one CSP, or unknowingly inheriting risk from an entire chain of invisible vendors?

Verified Primary CSP ✓ ✗ Invisible Vendor Chain

Interrogating Contractual Protections and Validating Independent Assurances

Point 13: Contractual Protection & Legal Terms

Crucial advisory area for MSMEs who routinely sign standard, non-negotiated cloud contracts.

CA's Core Question:
Does the contract allocate liability clearly, or does it leave the client completely exposed when trouble arrives?

Clear Responsibility ✓ ✗ Client Exposure

Point 14: Assurance Reports & Certifications

Certifications are highly useful, but auditors cannot treat vendor logos as automatic, blanket assurance.

CA's Core Question:
Do the assurance reports actually cover the specific service the client uses, or are they just brand-level certificates?

Service-Level Assurance ✓ ✗ Brand-Level Marketing

Securing User Identities and Ensuring Financial Reporting Reliability

Point 15: Access Management & Lifecycle Control

The vast majority of cloud risks originate from weak identity and access management.

CA's Core Question:
Can every single important action within the cloud system be definitively traced back to a properly authorized individual?

Traced Authorization | Anonymous Actions

Point 16: Application Controls & Reporting

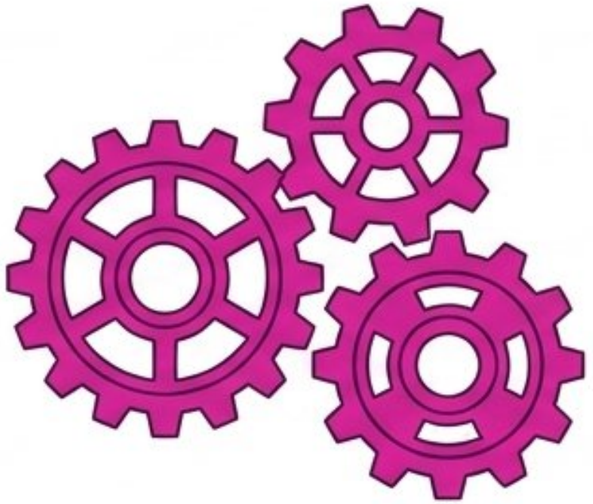
For a CA, this parameter is absolutely non-negotiable whenever cloud systems touch the books of account.

CA's Core Question:
Can the CA confidently rely on the workflows and reports generated by this system for formal audit and compliance purposes?

Reliable Audit Reports | Questionable Workflows

Managing Ecosystem Integration and Safe Operational Scaling

Point 17: Interoperability & Integration Risk

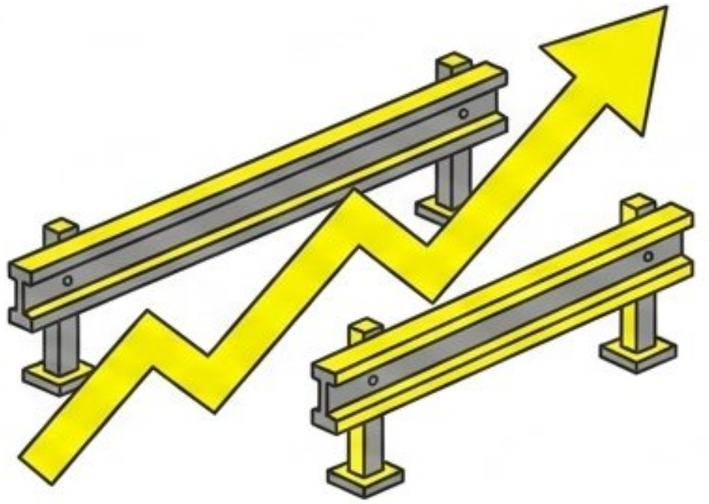


Cloud systems rarely operate in a vacuum; their connections to other tools often harbor hidden vulnerabilities.

CA's Core Question:
Does integrating this cloud system strengthen the overall control environment, or create hidden data leakage points?

✓ Strengthened Control ○ ✗ Hidden Leakage Points

Point 18: Scalability, Availability & Performance



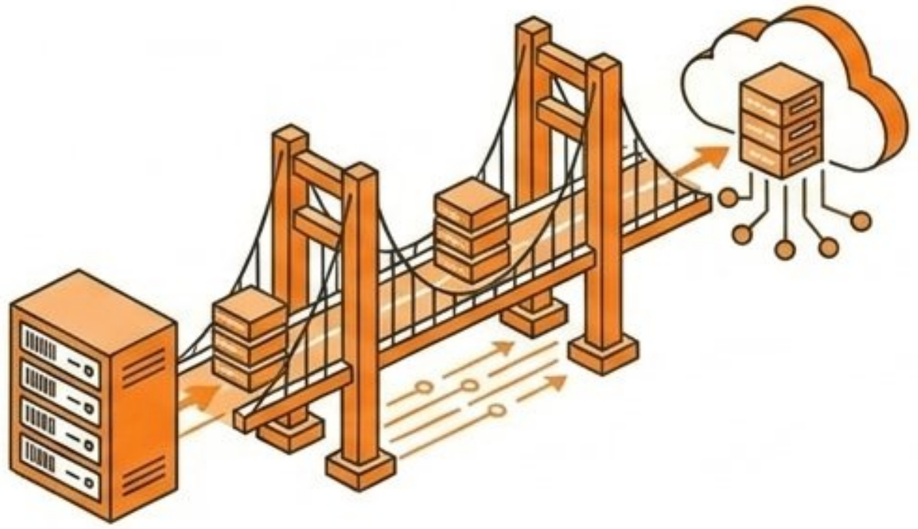
Particularly for MSMEs, cloud architecture must support rapid growth without sacrificing control or stability.

CA's Core Question:
Will the CSP reliably support the business's growth trajectory, or will increased load induce operational fragility?

✓ Supported Growth ○ ✗ Operational Fragility

Derisking the Extremes: Safe Migration and Unrestricted Exits

Point 19: Migration Risk & Implementation Quality



Data and operational failures are most likely to occur during the initial migration window, not post-go-live.

CA's Core Question:
Has the migration process strictly preserved data integrity and guaranteed unbroken business continuity?

✓ Preserved Integrity ✗ Migration Failure

Point 20: Exit Strategy & Vendor Lock-In

Entering the cloud is easy; a weak or undefined exit plan becomes a silent, expensive trap.

CA's Core Question:
Can the client cleanly leave the CSP without losing data, critical evidence, operations, or negotiating power?

✓ Safe Departure ✗ Silent Vendor Trap

The Ultimate Test: Management Visibility and The Diagnostic Matrix

Point 21: Governance, Reporting & Visibility

A superior CSP doesn't just execute operations; it actively empowers management to govern the ecosystem.

CA's Core Question:
Does the CSP provide transparent management visibility, or does it force the business to operate a black box?

✓ Management Visibility ○ ✗ The Black Box

The Cloud Accountability Matrix

Strategy & Finance

- Business Fit, TCO
- Reputation
- Scalability
- Migration
- Exit

Defense & Data

- Ownership, InfoSec
- Backup
- Access Management
- Interoperability

Law & Contracts

- Privacy (DPDP)
- Regulatory (RBI)
- Contracts
- SLA
- Assurance

Audit & Operations

- Logging (CERT-In)
- Incident Response
- Supply Chain
- App Controls
- Governance

The CA's definitive, one-page cheat sheet for client cloud audits.

The Governance Imperative

“The cloud is a powerful operational enabler, but governance is non-transferable.”

Technology can be outsourced; accountability cannot. Apply these 21 diagnostic checks rigorously to bridge the gap between cloud promises and audit realities.

Saurabh Maheshwari

Technology Simplified

+91 98292 03200 | saurabh@sklztect.com