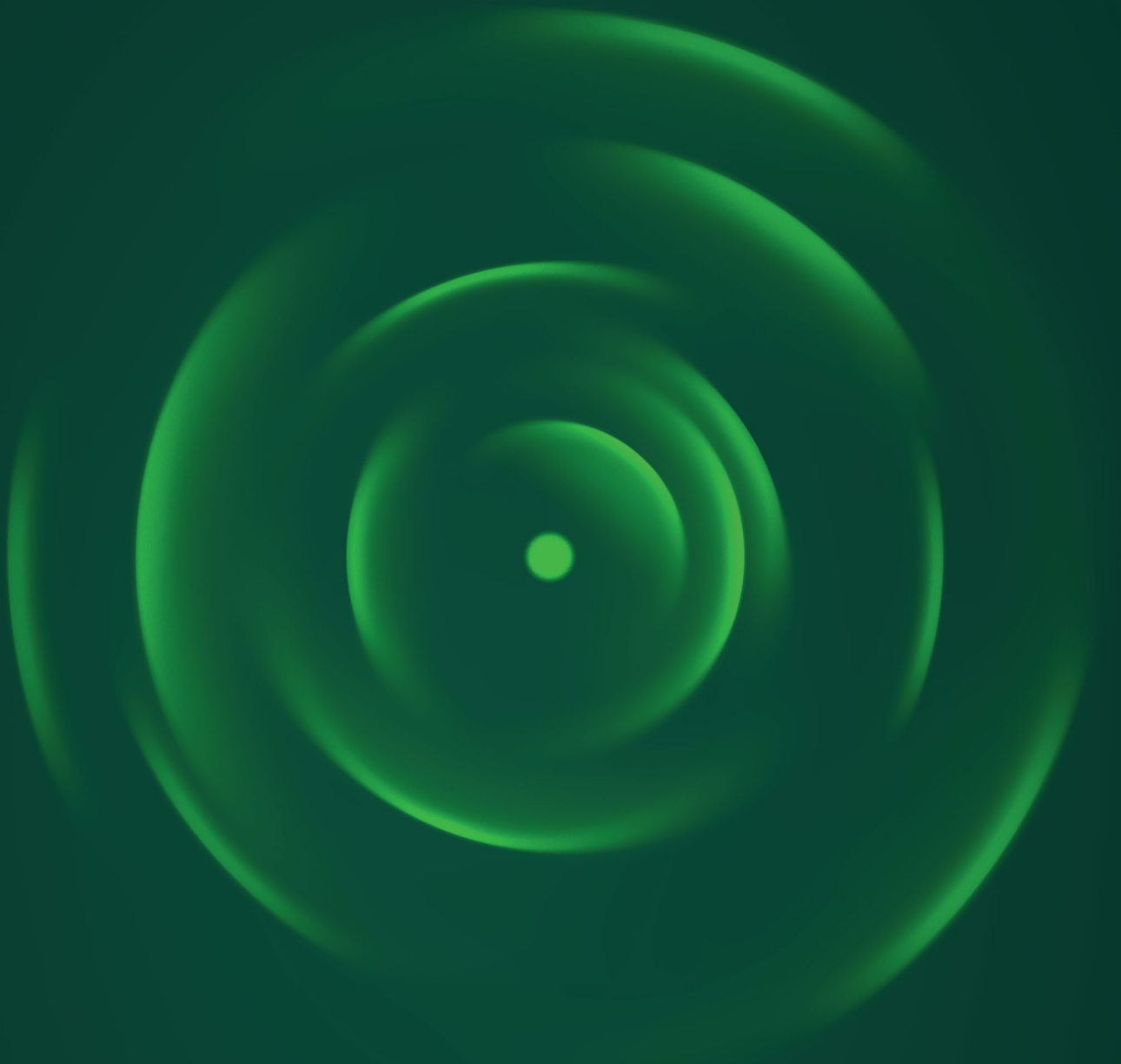
Deloitte.



Advisory lens: Navigating AI-related regulatory compliance

June 2026

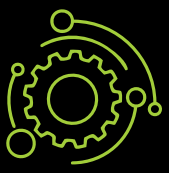
Table of contents

Introduction

Industries are undergoing substantial transformations led by rapid technological advancements, economic uncertainty and an evolving regulatory landscape. A key driver of this shift is the accelerated adoption of AI to enhance operational efficiency, decision-making and innovation.

However, this rapid integration of advanced AI tools, particularly in areas such as vulnerability detection, automation and cybersecurity, has introduced a new risk frontier. Regulatory bodies, including SEBI and the RBI, have raised concerns about the unintended consequences of AI adoption, including model vulnerabilities, data integrity risks, adversarial attacks and systemic financial threats.

According to **Deloitte's 2026 Future of Cyber Survey** and **AI risk insights,*** organisations are increasingly experiencing:



Surge in AI-driven cyber threats (e.g., automated exploitation, deepfake-enabled fraud, intelligent phishing).

Heightened exposure to third-party **AI tool risks** and **supply chain vulnerabilities.**

Growing reliance on AI without proportional governance, explainability and risk controls.

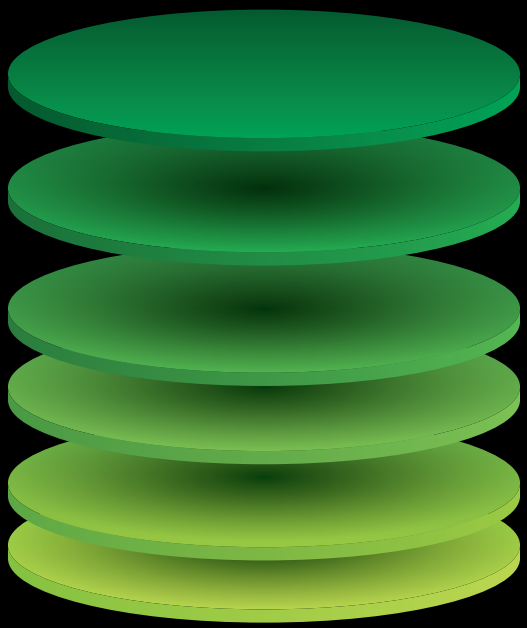
Increased concern over regulatory compliance and accountability gaps.

What is getting affected

Customer trust & brand reputation
Rising due to AI misuse and ethical concerns.

Regulatory compliance & governance
Lack of frameworks for AI accountability.

Operational resilience
Overdependence on AI-driven automation.



Cybersecurity posture
AI-enabled attacks evolving faster than traditional defences.

Financial systems stability
Algorithmic risks and cascading failures.

Data privacy & integrity
Misuse, leakage and manipulation of sensitive data.

*Deloitte Global 2026 Future of Cyber Survey | The State of AI in the Enterprise

AI-driven cybersecurity and regulatory risk advisory

AI is transforming industries at an unprecedented pace, but with innovation comes new responsibilities. AI is rapidly transforming cybersecurity and financial risk across India's financial ecosystem. SEBI and RBI are actively responding to this shift, balancing innovation with risk management.

Issued on 27 April 2026

RBI advisory

Advisory on advanced AI-related risks
Broader AI governance, systemic risk and financial stability across financial institutions.

Issued on 5 May 2026

SEBI advisory

Advisory on emerging advanced AI tools for vulnerability detection
AI-driven vulnerability discovery and exploitation risks in capital markets.

Highlights (SEBI + RBI)

- AI is accelerating risk beyond traditional control timelines.
- Expanding threat landscape across cyber, data and operations.

Key risk themes

AI as risk multiplier

Enables faster vulnerability discovery and cyberattacks.

Focus on resilience

Strong emphasis on patching, monitoring and testing.

Shift to machine-speed security

From periodic to continuous monitoring and response.

AI governance

Need for controls over AI usage, outputs and data risks.

Systemic risk

An interconnected financial ecosystem amplifies impact.

Collaboration and ecosystem approach

Shared intelligence, coordination and vendor oversight.

AI is shifting financial sector risk from human-scale to machine-scale, requiring continuous adaptive and coordinated resilience.

SEBI vs RBI – Converging regulatory focus on AI-driven cyber risk

SEBI addresses AI-driven cyber threat acceleration, while RBI focuses on governance and systemic risk together driving AI-resilient financial ecosystems.

SEBI
(Capital markets regulator)

AI-driven cyber threat acceleration in capital markets.

Key priorities

- Rapid vulnerability discovery and exploitation risk.
- Accelerated patching and AI-based vulnerability assessment.
- Continuous SOC/Market SOC monitoring and real-time response.
- API security, Zero Trust and system hardening.
- Cyber-suraksha.ai Task Force (SEBI-led AI cyber risk initiative).

AI-layered enhancement of cybersecurity controls.

RBI
(Banking and financial stability regulator)

AI governance, systemic risk and financial stability.

Key priorities

- AI governance framework (policy, lifecycle, accountability and human oversight).
- AI-specific threat controls (data poisoning, adversarial attacks, model risks).
- Data protection, privacy, auditability and output validation.
- Vendor and third-party AI risk management.
- Secure and responsible AI adoption policies.

Enterprise-wide AI governance and risk framework.

Regulatory positioning and supervisory expectation

Advisory nature

- No explicit compliance deadline.
- Effective upon issuance.
- Principle-based guidance.

Supervisory expectation

- Immediate alignment expected.
- Integrated into governance and risk frameworks.
- Evaluated through audits, inspections and supervisory reviews.

Note: The "SEBI circular (HO/13/19/12(1)2026-ITD- 1_CIMGI/10873/2026)" issued on May 5, 2026, and "RBI Advisory (April 27, 2026)" are explicitly "advisories", not prescriptive regulations with a mandated implementation deadlines for Compliance.

Operating model shift: Traditional to AI-driven cyber resilience

SEBI's machine-speed cyber expectations and RBI's AI governance focus together require a fundamental transformation in cyber operating models.

Traditional model Traditional cybersecurity	**AI-driven model** AI-driven cyber resilience
AI-Driven transformation	
• **Periodic vulnerability assessment** Scheduled scans and assessments.	• **Continuous, AI-assisted detection** Real-time discovery of threats and vulnerabilities.
• **Reactive SOC monitoring** Alerts reviewed after occurrence.	• **Real-time, predictive monitoring** AI/ML-driven analytics and proactive alerting.
• **Manual incident response** Human-driven investigation and response.	• **Automated/AI-assistance response** SOAR-led orchestration and autonomous actions.
• **Static risk assessments** Periodic, point-in-time risk evaluation.	• **Dynamic, real-time risk intelligence** Continuous risk scoring and threat intelligence.
• **IT-lead governance** Limited board-level oversight.	• **Board-led AI governance** Policy, accountability and strategic oversight.
• **Entity-focused security** Siloed controls within organisation.	• **Ecosystem-wide resilience** Collaboration security.

Cybersecurity is shifting from a control function to a real-time, AI-enabled strategic capability.

Faster detection

AI-driven visibility at machine speed.

Stronger response

Automated, intelligent and adaptive.

Greater resilience

Collaborative and ecosystem-wide.

Securities and Exchange Board of India (SEBI)

Advisory on emerging advanced AI tools for vulnerability detection

Advisory on emerging advanced AI tools for vulnerability detection – Need of the hour

AI is reshaping vulnerability discovery from human-scale to machine-speed, fundamentally altering cyber risk dynamics. The advisory is intended to be read in conjunction with SEBI CSCRF and related cybersecurity guidelines.

Why
(Need for advisory)

AI is accelerating cyber risk beyond traditional controls, requiring faster, more coordinated and more adaptive security.

- **Drivers:** Rise of AI-powered vulnerability tools, faster and more sophisticated cyber threats and the need for sector-wide coordinated resilience.
- **Speed risk:** Vulnerabilities can be found and exploited faster than they can be fixed.
- **Systemic risk:** An interconnected ecosystem can amplify a single weakness.
- **Data risk:** AI may impact confidentiality, integrity and reliability.
- **Dual-use risk:** Same AI tools can defend and attack.

Who
(Applicability)

The advisory applies to SEBI Regulated Entities (REs), including:

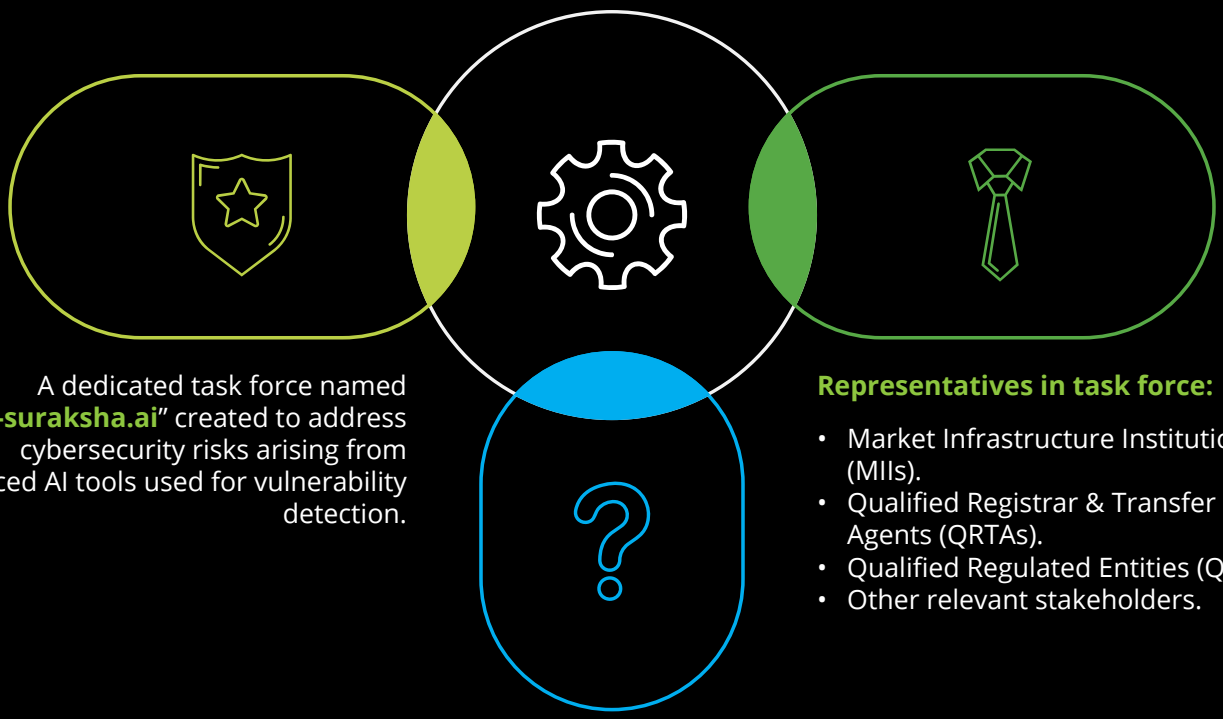
- Stock exchanges, clearing corporations and depositories.
- Stockbrokers, portfolio managers.
- Mutual funds/AMCs.
- AIFs, merchant bankers.
- Custodians, KRAs, credit rating agencies.
- Other intermediaries across the securities ecosystem.

What
(Key mandates and expectations)

SEBI expects organisations to move from periodic, reactive security to continuous, AI-aware and collaborative cyber resilience.

- **Faster security ops**: Rapid patching + continuous SOC monitoring.
- **AI-driven defence**: Use AI for vulnerability detection and risk assessment.
- **Stronger controls**: Zero trust, system hardening, secure APIs, vendor risk.
- **Continuous testing**: Regular VAPT, red teaming, AI threat scenarios.
- **Collaborative security**: Share threat intelligence and quickly report incidents.
- **Strategic shift**: Build long-term AI-led cyber resilience + align with market SOC.

Creation of “Cyber-suraksha.ai” task force



A dedicated task force named “**Cyber-suraksha.ai**” created to address cybersecurity risks arising from advanced AI tools used for vulnerability detection.

Representatives in task force:

- Market Infrastructure Institutions (MIIs).
- Qualified Registrar & Transfer Agents (QRTAs).
- Qualified Regulated Entities (QREs).
- Other relevant stakeholders.

SEBI observed that AI-driven tools can rapidly identify vulnerabilities, which creates risks such as:

- Faster exploitation of system weaknesses.
- Data confidentiality concerns.
- Reliability/integrity issues in AI outputs.

Key objectives of the task force

Assess AI-driven cybersecurity risks

- Study risks posed by AI-based models.
- Develop standardised mitigation strategies.

Strengthen incident reporting

- Ensure priority reporting of cyber incidents, attack vectors and vulnerabilities.
- Improve overall cyber resilience of the securities market.

Enable threat intelligence sharing

- Share information about vulnerabilities and threats.
- Disseminate best practices and response frameworks.
- Provide playbooks for handling attacks.

Review third-party cybersecurity

- Evaluate the security posture of third-party vendors and service providers.
- Including empanelled vendors used by regulated entities.

SEBI's key considerations for all industry sectors

The SEBI advisory is primarily aimed at securities market participants and provides recommendations on emerging advanced AI tools; however, it has broader applicability across industries and should be considered in conjunction with relevant SEBI cybersecurity and resilience circulars (such as SEBI CSCRF) and related updates.

Immediate patching and vulnerability management

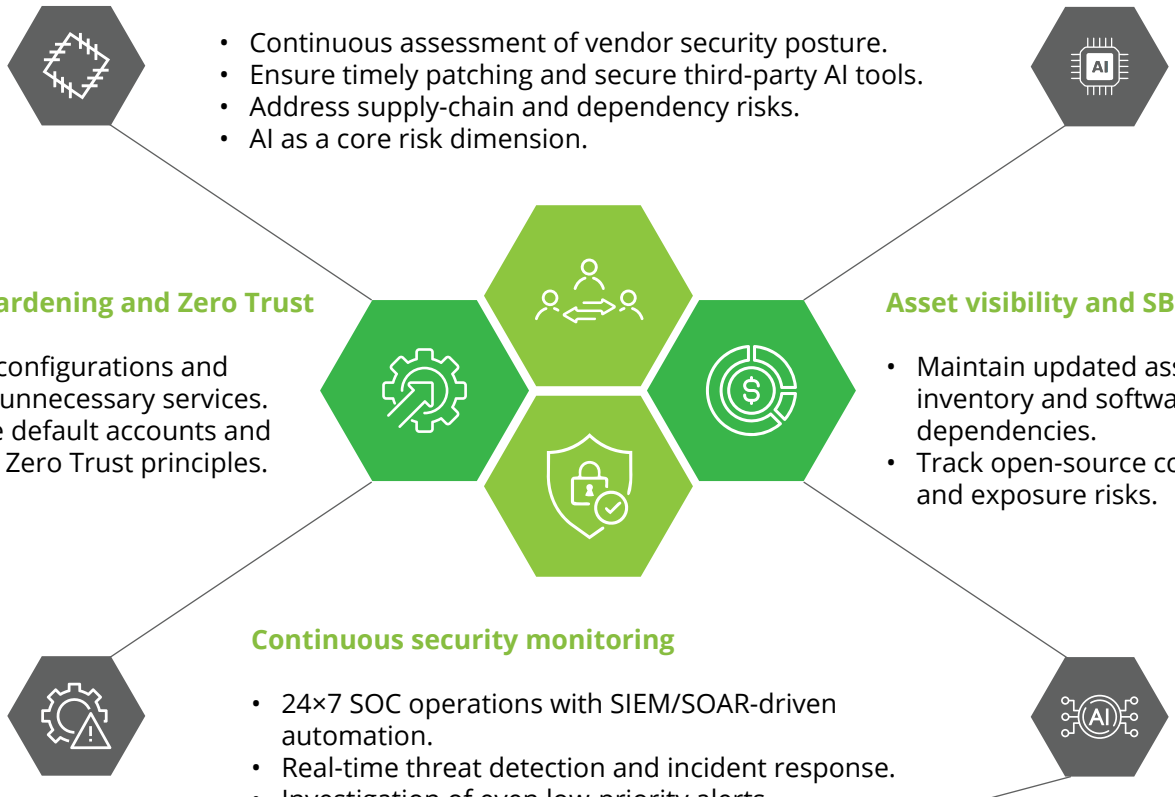
- Rapid patching and remediation of identified vulnerabilities.
- Well-defined scope and resources.
- Continuously assess systems for vulnerabilities using conventional and AI-assisted tools.

AI governance and oversight

- Validate reliability and integrity of AI outputs.
- Prevent unsafe or autonomous AI actions.
- Establish structured AI risk governance frameworks.
- Perform regular/continuous security audits.

Third-party and vendor risk management

- Continuous assessment of vendor security posture.
- Ensure timely patching and secure third-party AI tools.
- Address supply-chain and dependency risks.
- AI as a core risk dimension.



System hardening and Zero Trust

- Secure configurations and disable unnecessary services.
- Remove default accounts and enforce Zero Trust principles.

Asset visibility and SBOM

- Maintain updated asset inventory and software dependencies.
- Track open-source components and exposure risks.

Continuous security monitoring

- 24×7 SOC operations with SIEM/SOAR-driven automation.
- Real-time threat detection and incident response.
- Investigation of even low-priority alerts.

Risk assessment and scenario testing

- Include AI-driven threats in cyber risk assessments.
- Conduct scenario-based cyber simulations and drills.

Long term AI-enabled cyber defence

- Build AI-augmented detection and response capabilities.
- Move towards automated, machine-speed cyber resilience.

Strong API security

- Maintain updated API inventory.
- Implement strong authentication and least-privilege access.
- Enforce rate limiting, throttling and whitelist-based access.

SEBI – AI Cyber resilience roadmap

Enable safe, ethical and scalable AI adoption while safeguarding financial stability, consumer protection and systemic resilience.

Short term (0–90 days)

- Conduct an AI-focused vulnerability assessment.
- Review patching SLAs and backlog.
- Strengthen API security posture.
- Onboard/integrate with Market SOC.

Medium term (3–9 months)

- Implement AI-enabled threat detection.
- Enhance zero-trust architecture.
- Perform AI scenario-based cyber drills.

Long term (9–18 months)

- Build AI-aware cyber operating model.
- Embed AI governance frameworks.
- Align fully with SEBI CSCRF + AI Advisory.

Reserve Bank of India (RBI)

Advisory on advanced AI-related risks

RBI advisory on advanced AI-related risks

RBI emphasises AI-driven cyber resilience, governance-led oversight and ecosystem-wide risk management against emerging machine-speed threats.

Why
(Need for RBI intervention)

AI is amplifying cyber, operational and systemic risks beyond traditional security controls.

- **Model risk**: Bias, opacity and non-deterministic outcomes.
- **Cybersecurity threat**: Adversarial AI, data poisoning and deepfake-enabled attacks.
- **Systemic risk**: Herding effects, model convergence and procyclicality across financial markets.
- **Third-party risk**: Dependency on external AI vendors, cloud platforms and service providers.
- **Consumer risk**: Lack of explainability, unfair outcomes and reduced transparency in AI-driven decisions.
- **Data risk**: Privacy breaches and misuse of sensitive financial and customer data.

RBI highlights that AI can amplify cyber and systemic risks at machine speed.

Who
(Applicability)

The advisory applies across RBI-regulated entities and the broader financial ecosystem.

- Scheduled commercial banks.
- Small finance banks.
- Payments banks.
- NBFCs.
- Payment system operators.
- FinTech and digital partners.
- Third-party technology and infrastructure vendors.

RBI's focus extends beyond institutions to ecosystem-wide AI resilience.

What
(Key regulatory expectations)

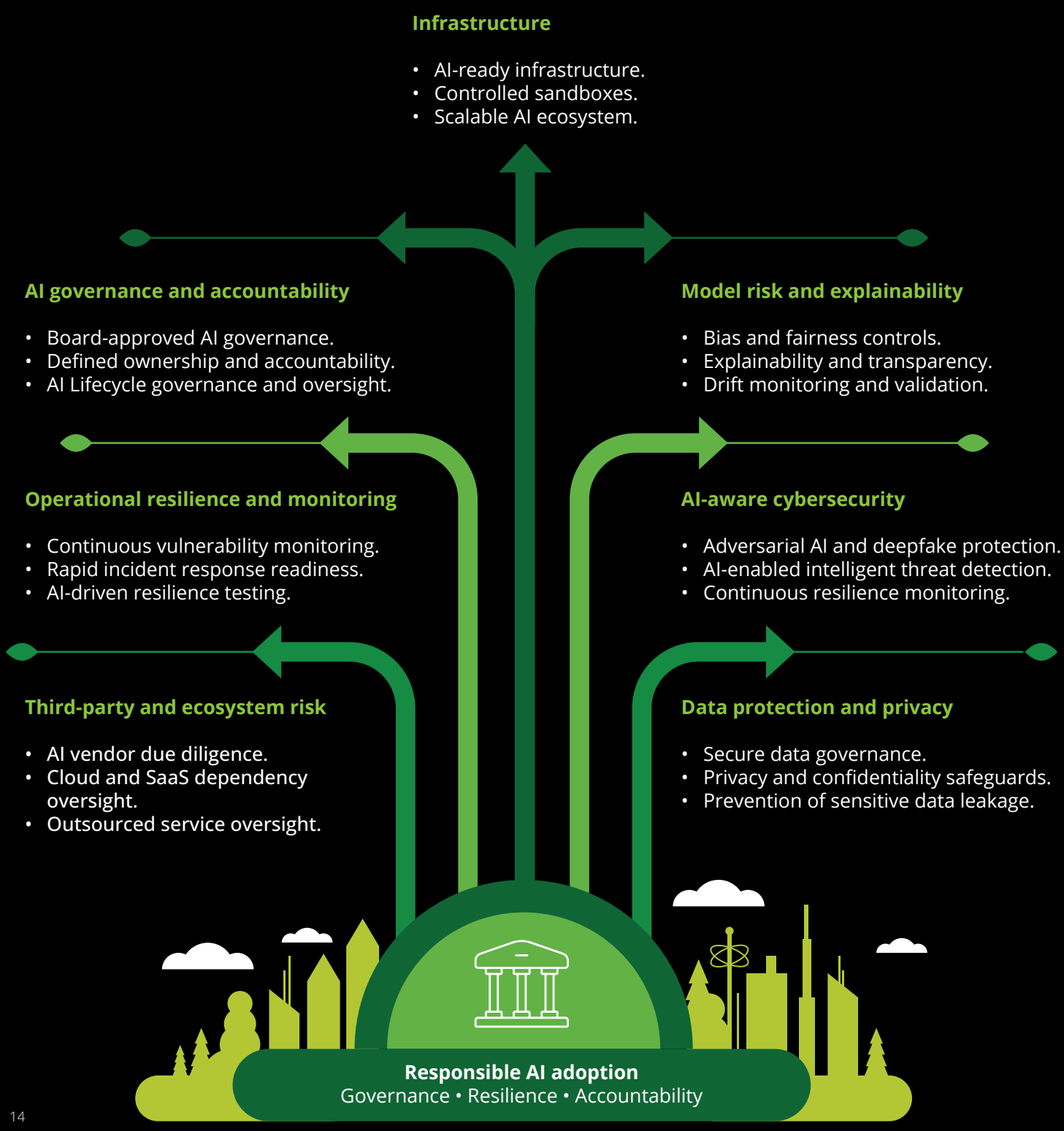
RBI expects financial institutions to adopt AI frameworks that are governed, explainable, resilient and continuously monitored.

- **AI governance and accountability**: Board-led oversight and lifecycle governance.
- **AI-aware cybersecurity resilience**: Protection against adversarial AI and deepfake-enabled threats.
- **Continuous monitoring and response**: Real-time detection and rapid incident response.
- **Accelerated vulnerability management**: Faster patching and continuous resilience testing.
- **Third-party and ecosystem oversight**: Governance over AI vendors, cloud and external dependencies.
- **Controlled AI usage and safeguards**: Secure AI adoption and prevention of sensitive data leakage.

RBI positions AI risk as a governance, cyber resilience and financial stability challenge across the banking ecosystem.

RBI – Key considerations for responsible AI adoption

RBI emphasises governance-led, explainable, resilient and risk-aware AI adoption across the banking ecosystem.



RBI – AI cyber resilience roadmap

Enable safe, ethical and scalable AI adoption while safeguarding financial stability, consumer protection and systemic resilience.

Short term (0–60 days)

- Conduct AI-focused cyber risk assessment.
- Review critical vulnerabilities and patch backlog.
- Present findings to board.
- Identify high-risk vendor dependencies.

Medium term (3–9 months)

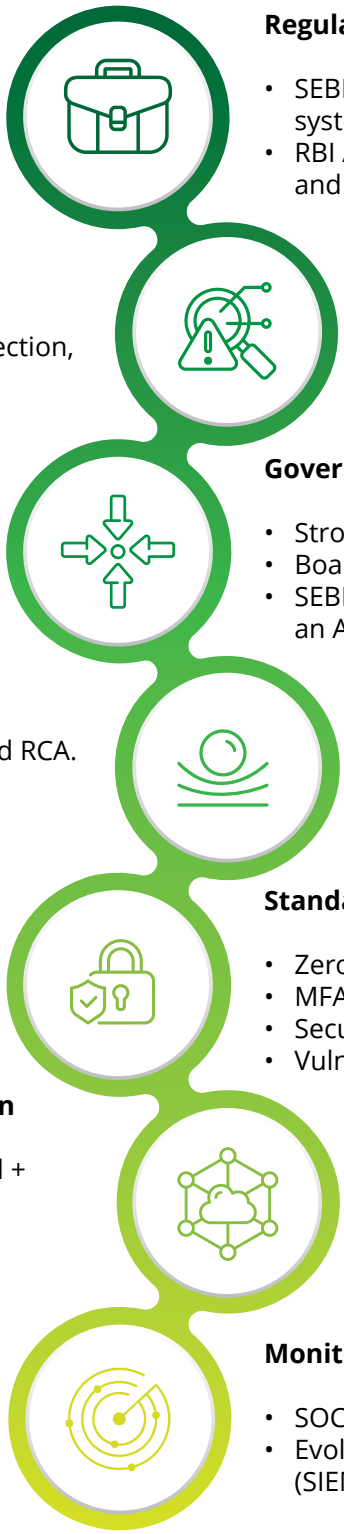
- Upgrade SOC and monitoring capabilities.
- Strengthen third-party risk frameworks.
- Implement continuous vulnerability scanning.
- Introduce AI-aware cyber scenarios.

Long term (9–18 months)

- Build AI-enabled cyber defence.
- Move towards:
  - Automated threat detection.
  - Predictive risk analytics.
- Align with RBI's broader FREE-AI governance principles.

Way forward

Responsible AI governance: Aligning SEBI and RBI frameworks



Regulator Positioning

- SEBI AI advisory highlights AI-driven systemic risks.
- RBI AI advisory enables deep AI governance and controls.

Risk and threat evolution

- Shift to a resilience-led approach.
- Inclusion of AI threats (prompt injection, model manipulation).
- AI as a core risk dimension.

Governance alignment

- Strong governance and accountability.
- Board-driven oversight across regulators.
- SEBI mandate IT Committees & RBI mandates an AI governance framework to cover AI risks.

Resilience and response

- Structured incident lifecycle + rapid RCA.
- AI-driven scenarios (deepfake, automated attacks).
- Forensics analysis.

Standardised security architecture

- Zero trust.
- MFA and least privilege.
- Secure-by-design systems.
- Vulnerability and patch management.

Data and ecosystem risk expansion

- Data protection → data + AI model + prompt security.
- Data protection and monitoring emphasis.
- AI supply chain risk.

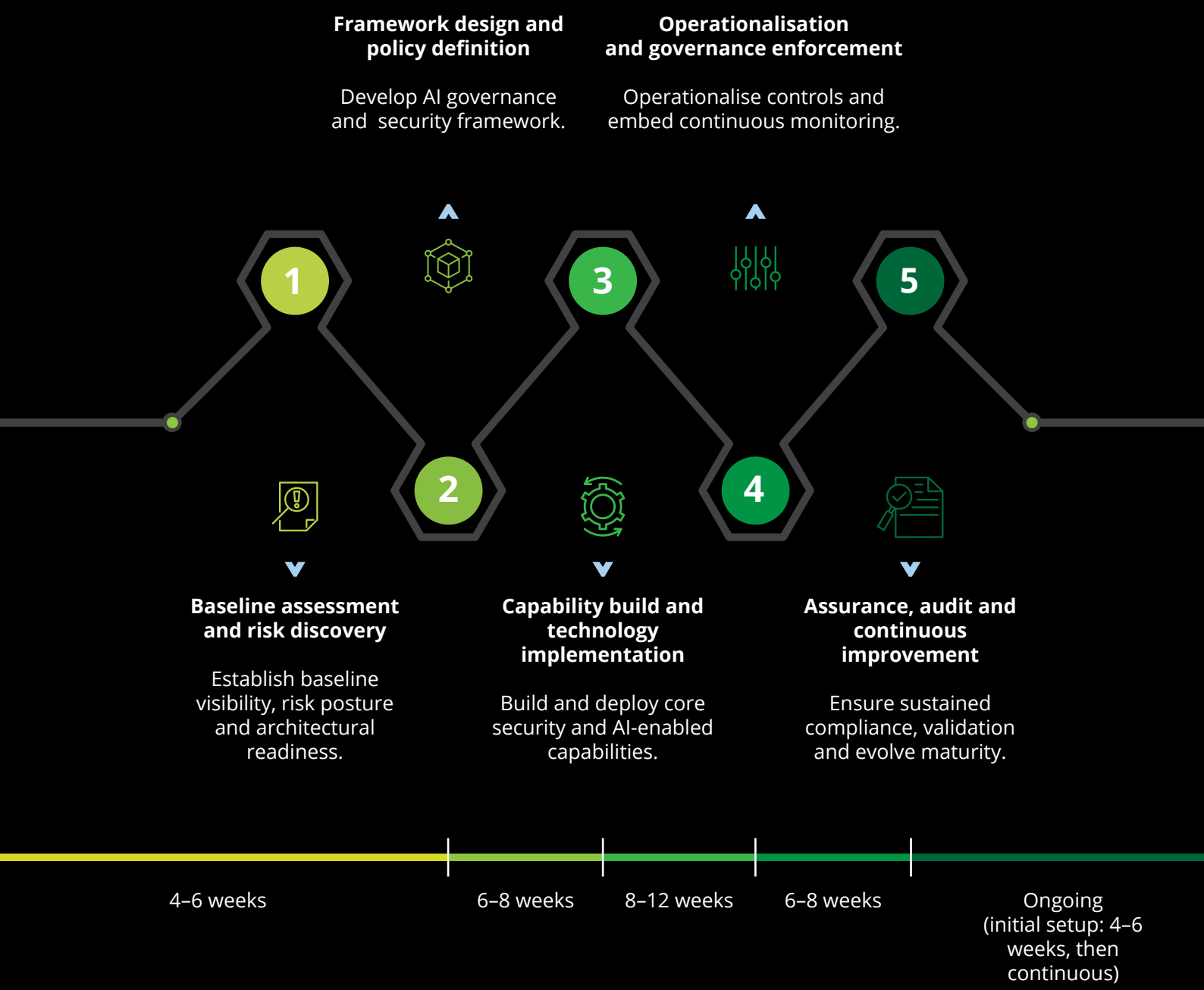
Monitoring and detection

- SOC becomes a central pillar.
- Evolution towards AI-augmented detection (SIEM, SOAR, XDR).

Regulatory convergence is driving a unified model combining cybersecurity, AI governance and ecosystem resilience, anchored on Zero Trust, continuous monitoring and risk-based controls.

Way forward for AI regulations

While SEBI and RBI guidelines apply within India, the global standards, frameworks and regulations, such as ISO 42001 (AIMS), NIST AI RMF, EU AI Act, GDPR and DPDP Act, provide a strong baseline for AI governance, with the way forward being to align these standards with local regulatory requirements for a comprehensive compliance approach.



Connect with us

Sathish Gopalaiah
President, Consulting
Deloitte South Asia

sathishtg@deloitte.com

Gaurav Shukla
Partner and Leader - Cyber
Deloitte South Asia

shuklagaurav@deloitte.com

Deepa Seshadri
Partner
Deloitte India

deseshadri@deloitte.com

Munjal Kamdar
Partner
Deloitte India

mkamdar@deloitte.com

Ashish Sharma
Partner
Deloitte India

sashish@deloitte.com

Vikas Garg
Partner
Deloitte India

vikasgarg@deloitte.com

Contributors

Megha Goyal
Sulekha Kumari

Deloitte.