www.inductusgcc.com

IRRESISTIBLE INDIA

CYBER RESILIENCE BY DESIGN

Rethinking Security Architecture for AI-Driven GCCs

2026

Inductus Research

executive SUMMARY

2,100+

GCCs Opening in India, 2025

94.4%

of AI agents vulnerable to prompt Injection

$4.4M

average global cost of a data breach,2025

India alone hosts over 2,100 Global Capability Centers/Offshore Delivery Centers today, part of a global GCC/ODC market valued near USD 601 billion in 2025 and projected to reach USD 886 billion by 2030. Roughly 110 new centers were established in India between 2024 and 2025, and 83% of GCCs/ODCs are now scaling generative AI projects while 58% are actively investing in agentic AI. This scale of adoption is a strategic win for the enterprises that own these centers, but it also means every GCC is quietly becoming one of the largest AI attack surfaces inside the global enterprise.

Security has not kept pace. Only 42% of GCCs/ODCs operate advanced or automated cybersecurity frameworks, and just 7% have a fully embedded security center of excellence. Meanwhile, the underlying AI systems these centers are deploying are structurally fragile: independent research shows 94.4% of tested large language model agents are vulnerable to prompt injection, and 100% are vulnerable to inter-agent trust exploits. Globally, 63% of organizations still operate without any AI governance policy, and 97% of organizations that suffered an AI-related breach had no proper AI access controls in place.

The financial stakes are concrete. IBM's 2025 Cost of a Data Breach Report puts the global average breach cost at USD 4.44 million, rising to USD 4.63 million when shadow AI is involved and to USD 10.22 million in the United States. Regulators are moving in parallel: India's DPDP Act has entered an enforcement heavy phase, SEBI's Regulation 16C now places strict responsibility for AI outputs on regulated entities, RBI's FREE-AI framework is shaping financial sector AI governance, and CERT-In mandates incident reporting within six hours of detection.

This report makes the case that security can no longer be layered on top of AI systems after deployment. It proposes a seven-layer security-by-design architecture built specifically for AI-driven GCC/ODC environments, benchmarks current GCC/ODC cybersecurity maturity against a four-stage resilience model, and sets out a practical roadmap so GCC and business leaders can get ahead of regulatory mandates rather than react to them.

TABLE OF CONTENT

The Expanding Attack Surface

How AI Is Reshaping GCC Risk

Traditional GCC security programs were built to defend applications, endpoints, and networks. AI adoption adds three new categories of exposure that most existing programs were never designed to address: the model itself can be manipulated, autonomous agents can be tricked into misusing their own permissions, and agents talking to other agents can propagate an attack far beyond its point of origin.

1.1 Model Manipulation Is Already Happening at Scale

Prompt injection is now recognized by OWASP as the number one critical vulnerability for large language model applications in its 2025 Top 10 for LLM Applications, and the data backs that ranking up. A 2025 benchmark study found that 94.4% of tested AI agents could be hijacked not through a conventional software exploit or a stolen credential, but simply through the content they were asked to read: an email, a support ticket, a shared document, or a web page. Because agents act on an organization's behalf across systems, a successful injection is not an embarrassing bad reply, it is unauthorized data leaving the enterprise, messages sent in the company's name, and systems changed without approval.

Structural Fragillity of Today's LLM Agents (Independent Benchmarks, 2025)

Fig. 1: Independent 2025 benchmarks of LLM agent susceptibility to manipulation.

Academic red teaming reinforces the scale of the problem. One black box injection technique compromised 31 of 36 real-world LLM-integrated applications at an 86.1% success rate. A separate tool poisoning technique reached up to 96.7% attack success against tool-selecting agents, and a mixed attack strategy averaged 84.3% success across thirteen different model backbones. Direct injection attacks against contemporary web agents succeeded more than 79% of the time in a 2026 study, even against current-generation frontier models.

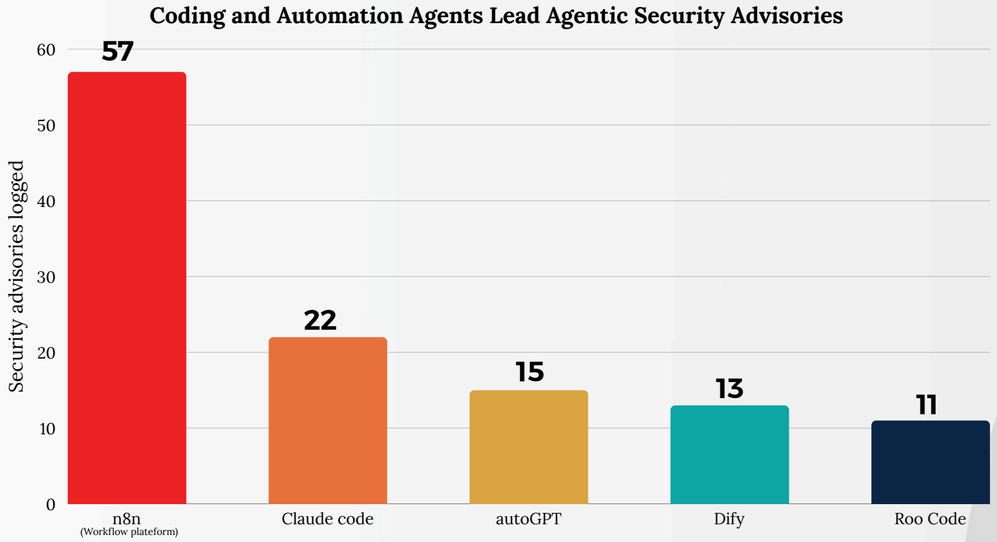
1.2 Agent to Agent Vulnerabilities: A New Class of Systemic Risk

As GCCs move from single-purpose chatbots to fleets of autonomous agents that plan, call tools, and hand off tasks to one another, the attack surface stops being a set of discrete applications and becomes a connected system. A single well-placed injection can self-replicate across interconnected agents in a multi-agent system, behaving much like a computer virus and causing system-wide disruption rather than a contained incident.

This risk is compounding quickly. Gravitee's State of AI Agent Security survey of 750 technology executives found that AI agent fleets have roughly doubled since December 2025, while monitoring coverage, accountability structures, and pre-deployment controls have barely moved, meaning organizations are growing more comfortable with a risk they have not actually reduced. Darktrace's State of AI Cybersecurity 2026 report found that 92% of security professionals are concerned about the impact of AI agents on their organizations, and a Dark Reading poll found 48% of cybersecurity professionals now rank agentic AI and autonomous systems as the single most dangerous attack vector of the year.

Memory poisoning adds a further dimension unique to agentic systems: an adversary implants false or malicious information into an agent's long-term memory, and unlike a prompt injection that ends when a session closes, the poisoned instruction persists and can resurface weeks or months later, long after the original point of compromise has been forgotten.

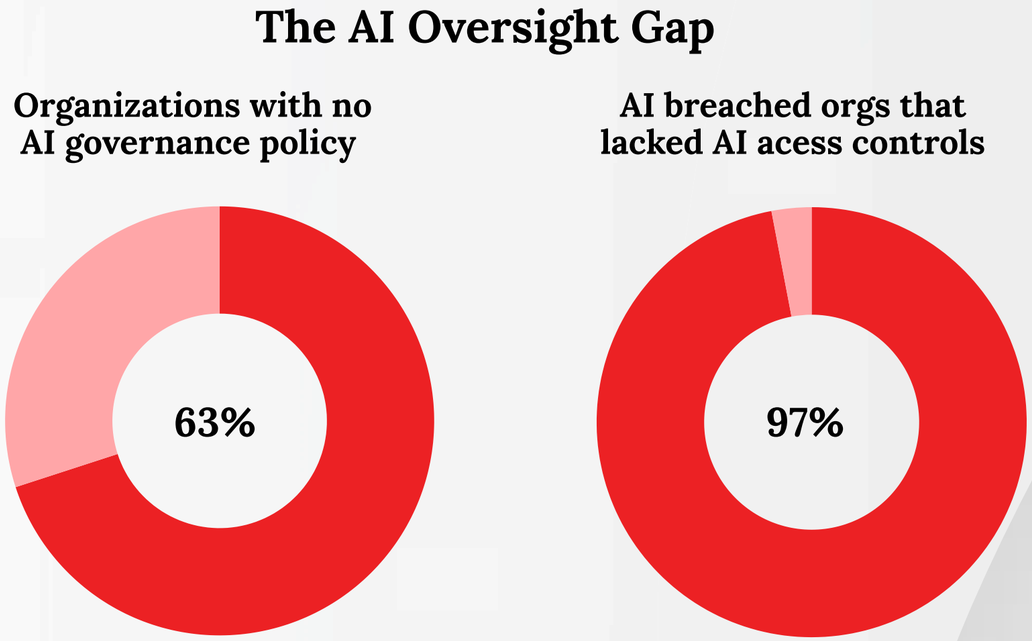
At the tooling layer, OWASP's tracking of 53 agentic AI projects found that coding and workflow automation agents generate the highest volume of security advisories, reflecting both their rapid adoption inside enterprise engineering teams and the immaturity of their security controls.



1.3 Shadow AI and the Governance Gap

Shadow AI, the use of AI tools without security or governance approval, has become a leading and largely invisible driver of breach cost. IBM's 2025 research found that shadow AI played a role in 20% of breaches, and separate research from Kiteworks found that **83%** of organizations operate without basic controls to prevent sensitive data from reaching AI tools in the first place. More than a quarter of organizations report that over **30%** of the data flowing through their AI systems contains private or sensitive information.

The consequences are asymmetric. Security incidents involving shadow AI led to personally identifiable information being compromised **65%** of the time, versus a global average of 53%, and intellectual property exposure of **40%** versus a global average of **33%.** Organizations with high shadow AI usage paid an average of USD 670,000 more per breach than those with low or no shadow AI exposure. For GCCs handling parent company financial data, source code, customer records, and proprietary models, this is precisely the profile of the asset most at risk.



Source : IBM Cost of a Data Breach Report 2025, Ponemon Institute

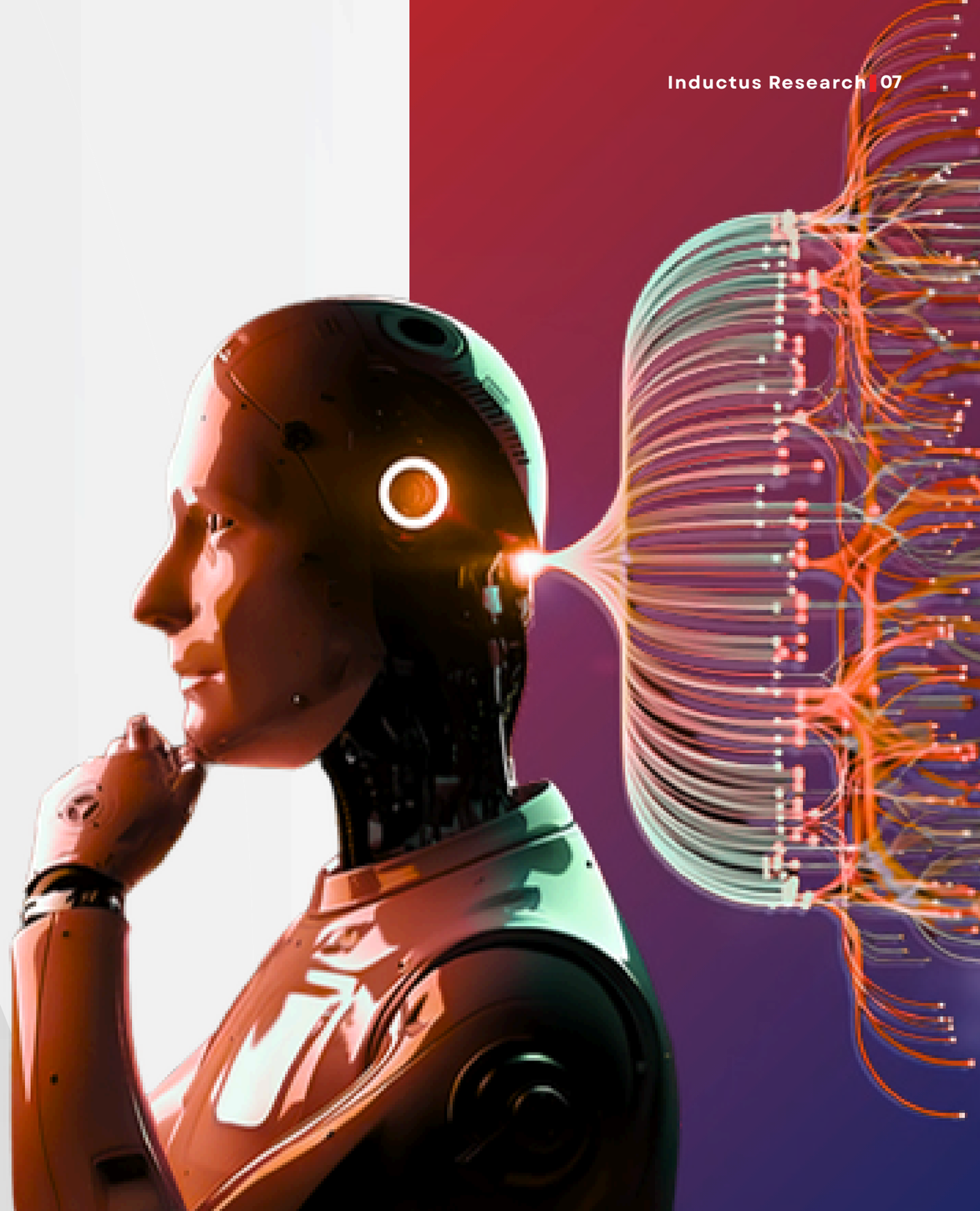
Fig. 3. The gap between AI adoption and AI governance is the single largest predictor of AI-related breach severity.

1.4 Identity, Deepfakes and the Erosion of Trust

Generative AI has also industrialized identity fraud. A September 2025 Gartner survey found that **62%** of organizations experienced a deepfake-enabled attack in the prior 12 months, **32%** faced an attack on AI applications through prompt manipulation, and **29%** experienced an attack directed at their enterprise generative AI infrastructure itself. Industry tracking suggests a deepfake-enabled fraud attempt now occurs somewhere in the world roughly once every five minutes.

The financial reality of this threat is not theoretical. In February 2024, attackers used a real-time deepfake video call impersonating a company's chief financial officer and other executives to defraud the Hong Kong office of engineering firm Arup of **USD 25.6 million** across fifteen separate wire transfers.

For GCCs that increasingly hold approval authority over payments, vendor onboarding, and system access on behalf of a global parent, synthetic identity attacks against video calls, voice authorization, and biometric checks are no longer an edge case; they are a mainstream fraud vector that identity verification systems built for a pre-AI world were not designed to catch.



1.5 Infrastructure and Supply Chain as Systemic Risk

AI has not eliminated traditional infrastructure risk; it has compounded it. IBM's 2025 data shows supply chain compromise accounted for 15% of breaches, at an average cost of USD 4.91 million, and these incidents took the longest of any category to detect and contain, 267 days on average, because they exploit trust relationships that conventional security tooling is not built to monitor.

Third-party involvement in breaches doubled year over year, from 15% to 30%, and 44% of zero-day attacks now target managed file transfer platforms, the very systems many GCCs use to move data between the AI tools, model providers, and outsourced partners in their delivery chain.

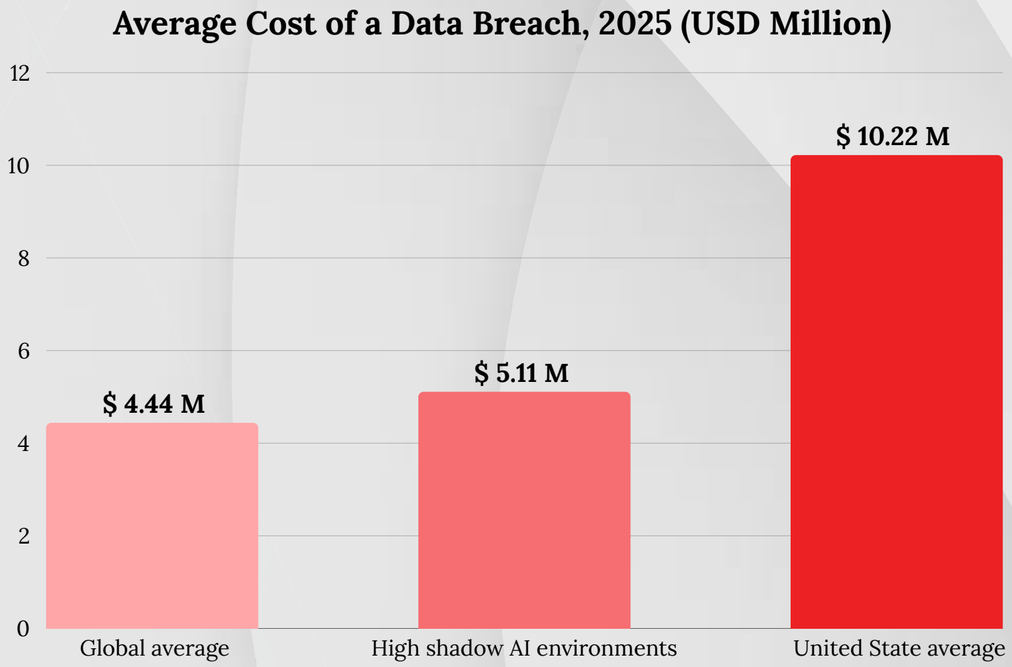
For a GCC, this risk is magnified by the sheer number of vendors, foundation model providers, plugin developers, data labeling partners, and cloud hosts that sit inside the AI supply chain.

A single unvetted model checkpoint, an unpatched plugin or an unmonitored third-party API can become the entry point for an attacker with no need to breach the enterprise's own perimeter at all.

1.6 The AI Talent Gap as a Security Constraint

Even well-intentioned GCC leaders face a structural constraint: there are not enough qualified people to secure what is being built. The global cybersecurity workforce gap reached a record **4.8 million** unfilled roles in 2025, up **19%** year over year, and organizations are filling only about **72%** of open security positions, leaving roughly one in four seats vacant. In ISC2's 2025 workforce study, AI security skills were cited as the single most pressing need by **41%** of respondents, ahead of cloud security, and **76%** of organizations openly acknowledge they cannot match the speed of AI-powered attacks with their current teams. **88%** of security teams report having experienced a real, tangible consequence directly attributable to a skills deficiency.

For GCCs, which are often asked to run global-scale security operations with regional hiring budgets, this gap is not an abstraction. It is the practical reason so many centers remain stuck operating legacy, rules-based controls even as the systems they are meant to protect become autonomous, generative, and self-directing.



1.7 What This Costs When It Goes Wrong ?

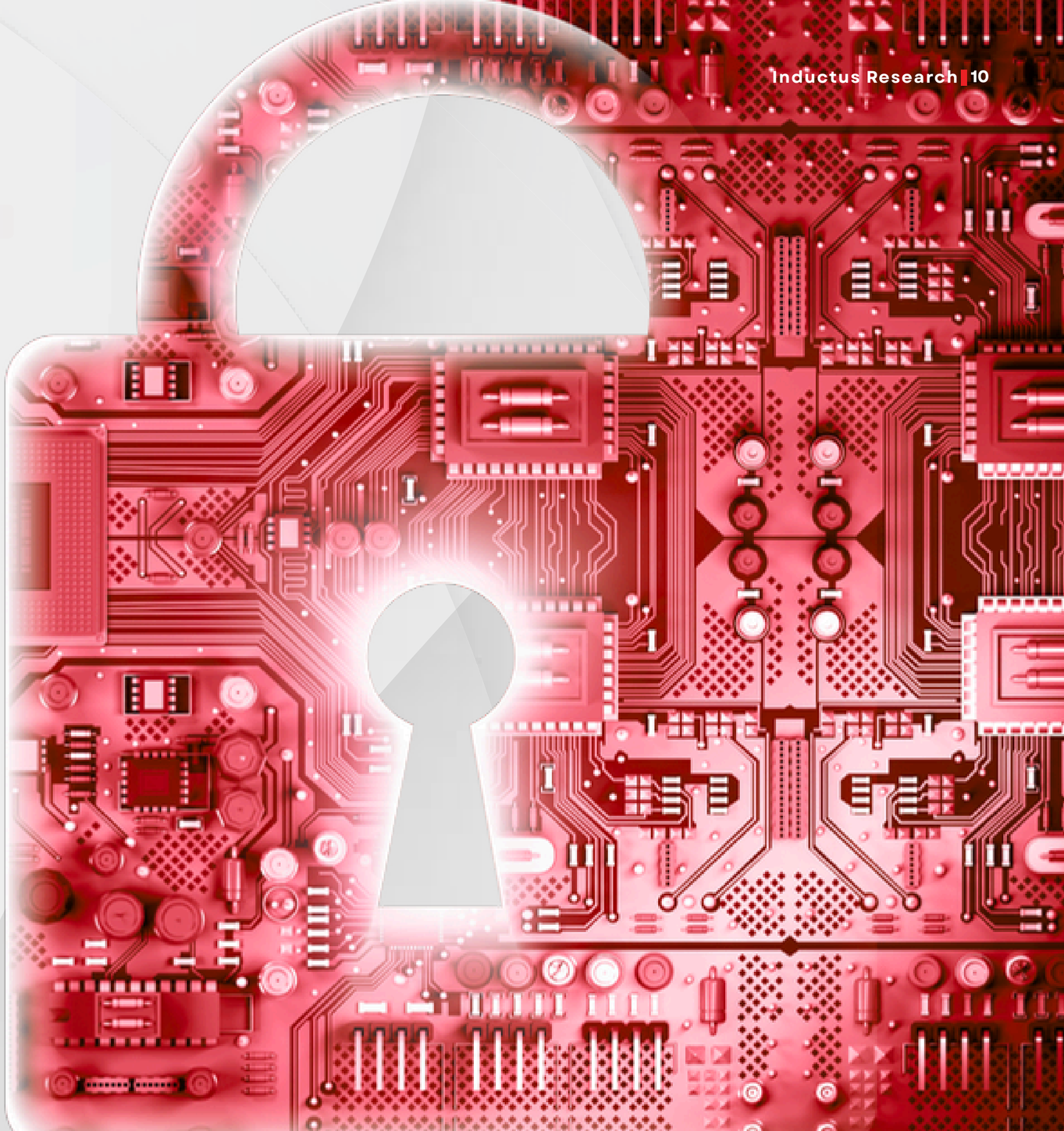
Every risk category above ultimately resolves into a single number that matters to a board: the cost of a breach. IBM and the Ponemon Institute's 2025 research puts the global average at USD 4.44 million, the first year-over-year decline in five years, driven largely by faster detection through security automation.

But that global figure masks two important divergences that GCC and business leaders should track closely.

First, organizations with high, ungoverned shadow AI usage paid meaningfully more, an additional USD 670,000 on average.

Second, the United States recorded a record USD 10.22 million average, a trend line that matters directly to Indian GCCs because so many serve US-headquartered parents whose breach costs, regulatory exposure, and litigation risk flow straight back to the center that touched the compromised data.

97% of organizations that suffered an AI-related breach had no proper AI access controls in place, and 63% had no AI governance policy of any kind, which means the overwhelming majority of this cost is preventable with the kind of structural controls.



Security by Design

An Architecture Framework for AI-Driven GCCs

Retrofitting security onto AI systems after deployment has proven both expensive and structurally insufficient. The alternative is to design security into every layer of the GCC's AI stack from the outset.

The framework below organizes AI security into seven layers, moving from board-level governance down through identity, data, models, agent orchestration, infrastructure, and finally detection and response. Each layer addresses a distinct category of risk, and together they form a defensible architecture that regulators, auditors, and enterprise security teams can assess consistently across a global GCC network.

Security by Design : A Layered Framework For AI Driven GCCs

01
Governance, Risk and Compliance Layer
Board oversight, AI policy, DPDP/RBI/SEBI/CERT-In alignment, model risk committees

02
Identity and Access Layer
Zero trust for humans, service accounts and AI agents: Just in time credentials,least privilege

03
Data Layer
Classification, lineage, encryption, data loss prevention for prompts, outputs and training sets

04
Model and Application Layer
Adversarial testing, guardrails, prompt injection defenses, output validation, red teaming

05
Agent Orchestration Layer
Agent to agent trust boundaries, tool permissioning, action approval workflows, memory intergrity checks

06
Infrastructure and Network Layer
A wonderful serenity has taken possession of my entire soul

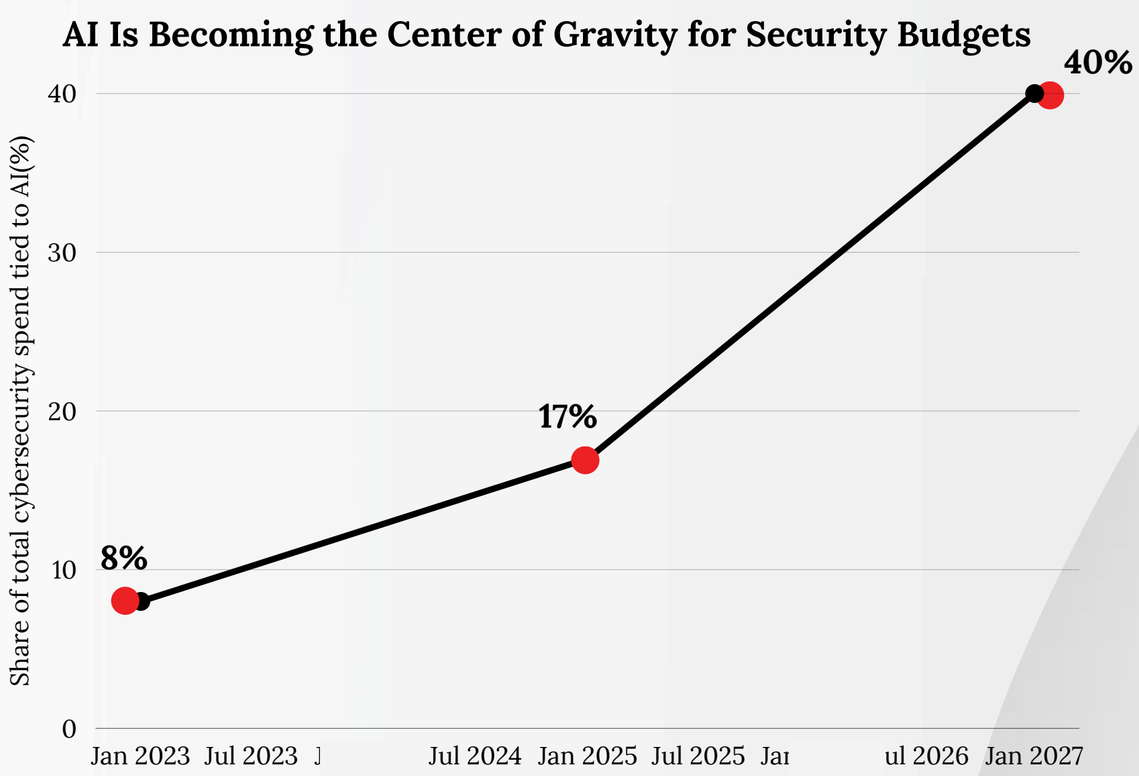
07
Detection, Reponse and Resilience Layer
AI-aware SOC, anomaly detection, incident playbooks, crisis simulation, continuous monitoring

2.1 Layer by Layer: Controls that Matter

Layer	Primary risk addressed	Representative controls
Governance, risk and compliance	Ungoverned AI adoption, regulatory exposure	AI use policy, model risk committee, DPDP / RBI / SEBI / CERT-In mapping, board reporting cadence
Identity and access	Compromised credentials, excessive agent privilege	Zero trust access, just-in-time credentials for agents, cryptographic signing of privileged commands
Data	Data leakage via prompts, outputs and training sets	Data classification, encryption, prompt and output level data loss prevention, retention controls
Model and application	Prompt injection, jailbreaks, adversarial manipulation	Input sanitisation, output validation, adversarial testing, continuous red teaming
Agent orchestration	Agent-to-agent trust exploits, memory poisoning	Trust boundaries between agents, tool permissioning, human in the loop approval for high-risk actions
Infrastructure and network	Lateral movement, insecure MLOps pipelines	Segmented environments, secure CI/CD for models, cloud security posture management
Detection, response and resilience	Delayed detection, uncontained incidents	AI-aware SOC, anomaly detection tuned to agent behaviour, tested incident response playbooks

2.2 Design Principles for GCC Leaders

- **Treat every AI agent as a new identity, not a feature:** it needs its own credentials, scoped permissions, and audit trail, the same discipline applied to a human employee or a service account.
- **Assume prompt injection will succeed sometimes:** design for containment through privilege separation and human approval on high-value actions, rather than relying on detection alone.
- **Close the technical control gap on shadow AI:** Only 17% of organizations currently have technical controls capable of preventing uncontrolled data flows into public AI tools, so policy alone is not enough.
- **Build governance that regulators can audit within 24 hours:** model cards, training data provenance, bias audit reports, and AI-specific breach response plans should be maintained continuously, not assembled after an incident.
- **Fund AI security proportionate to AI adoption:** Gartner forecasts that AI-related capabilities will account for more than 40% of total cybersecurity spending by 2027, up from just 8% in 2023, and GCCs that underinvest now will pay a steep catch-up premium later.

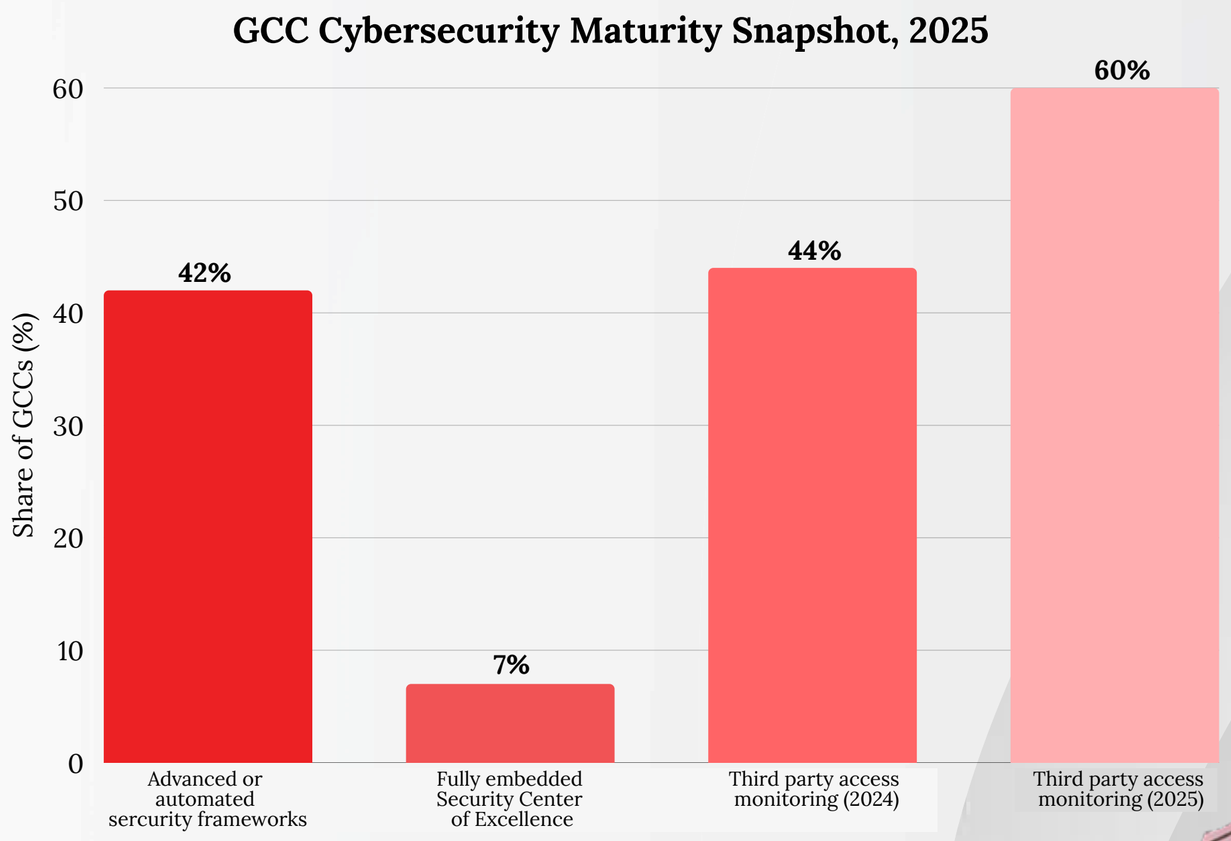


Benchmarking GCC Cybersecurity

Maturity and the Roadmap Ahead

Most GCCs are further along their AI adoption curve than their security maturity curve, and the gap between the two is where enterprise risk concentrates.

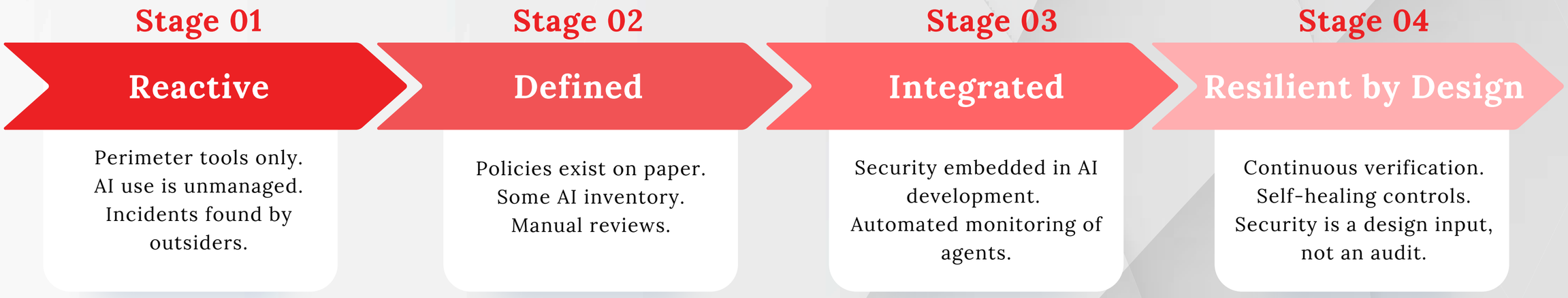
EY's GCC Pulse Report 2025 finds that cybersecurity maturity across GCCs remains moderate: **42%** of GCCs operate advanced or automated security frameworks, but only **7%** have a fully embedded security center of excellence with dedicated ownership of AI and cyber risk. On a more encouraging note, monitoring of third-party access has risen sharply, from **44%** of GCCs in 2024 to 60% in 2025, reflecting a broader shift toward zero-trust models and more proactive risk management.



Source: EY India GCC Pulse report 2025/ GCC Journal 2026

3.1 A Four-Stage Maturity Model for AI-Driven GCCs

Drawing on current GCC benchmarking data and the AI security literature reviewed in this report, GCC leaders can place their organization on a four-stage resilience curve. Most GCCs today sit between Stage 1 and Stage 2; the leading centers identified in industry benchmarking are already operating in Stage 3 and Stage 4, and that gap is widening fast enough to be a board-level conversation rather than a purely technical one.

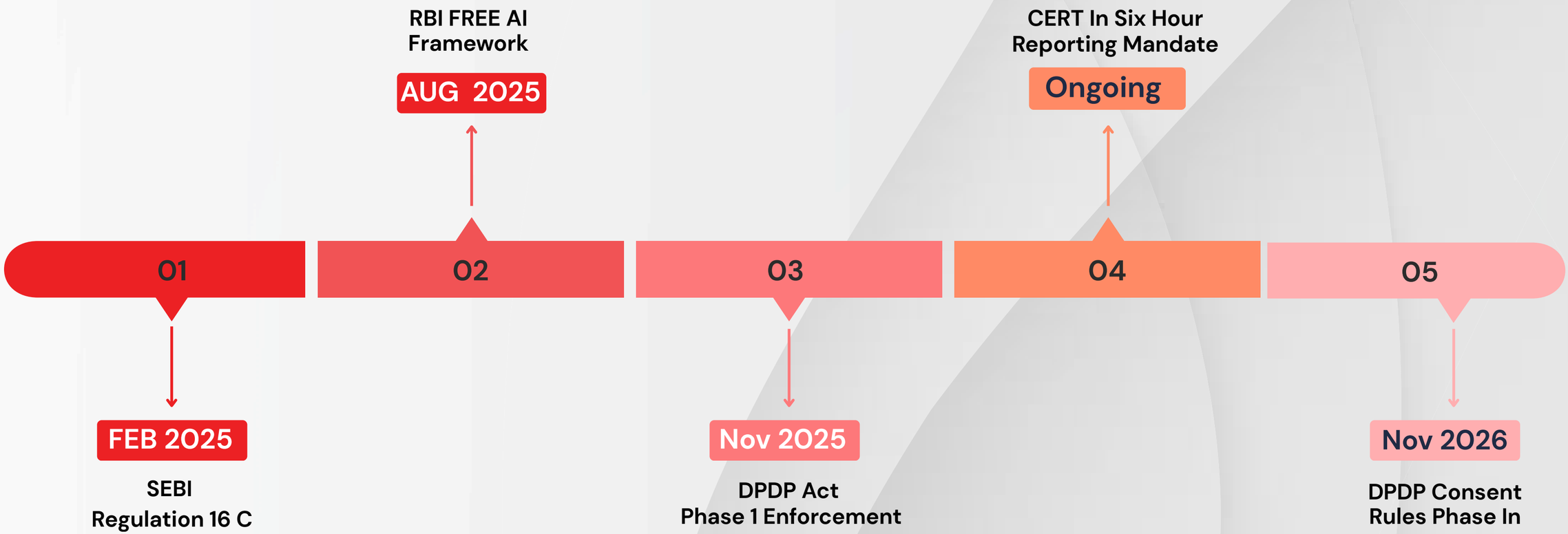


Stage	What It Looks Like	GCC Benchmark Signal
Stage 1: Reactive	Perimeter tools only. AI use across the center is largely unmanaged and undiscovered. Incidents are typically found by outsiders, auditors, customers, or the media, rather than by internal teams.	Where most GCCs and ODCs sit today, consistent with the finding that only **42%** operate advanced or automated security frameworks.
Stage 2: Defined	Written policies exist, and a partial AI inventory has begun, but enforcement is manual, ad hoc, and inconsistent across business units.	A center that has appointed an AI governance owner but has not yet automated controls.
Stage 3: Integrated	Security is embedded directly into AI development pipelines. Agents and models are monitored continuously, and incident response has AI-specific playbooks.	The transition phase where centers move from manual governance to automated, pipeline-integrated security controls.
Stage 4: Resilient by Design	Controls verify continuously rather than periodically. Systems can contain and self-correct many classes of AI-specific incidents automatically, and security metrics are reported to the board as a standing agenda item.	Fewer than **7%** of GCCs and ODCs have reached this stage, consistent with the finding that only **7%** report a fully embedded security center of excellence.

3.2 The Regulatory Mandates GCCs Should Get Ahead Of

India's regulatory environment for AI and data is moving from principle to enforcement, and GCCs that build for these requirements now will avoid a costly retrofit later.

India's AI and Data Regulatory Timeline Is Already in Motion

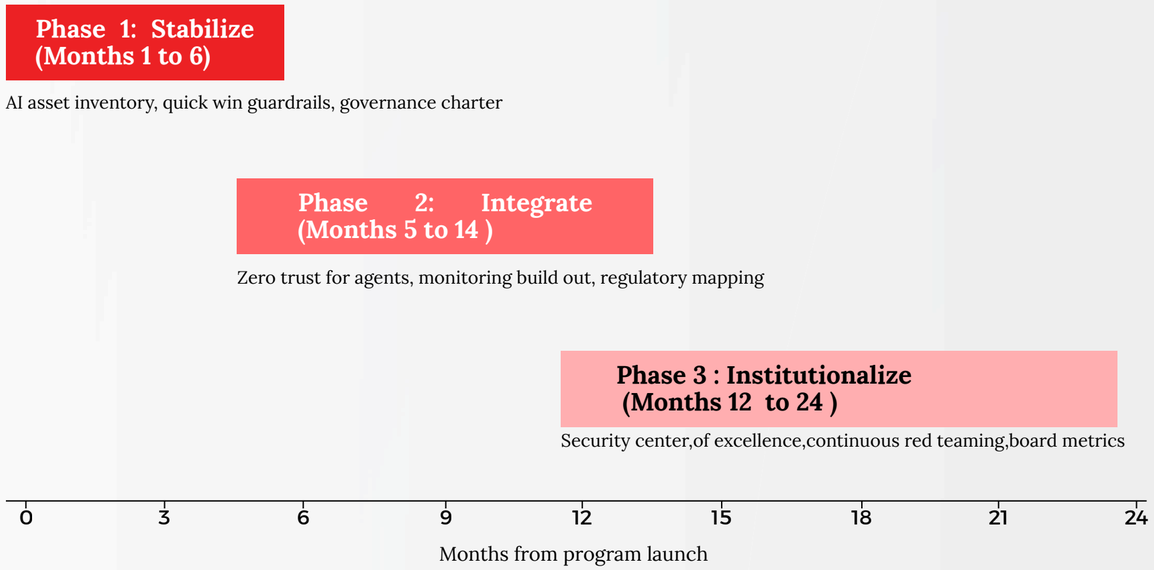


Regulation or framework	Scope	What it means for GCCs
DPDP Act, 2023	Personal data processed by any AI system covering Indian data principals	Entered an enforcement-heavy phase in 2026; mandatory, time-bound breach notification; compliance glide path continues toward 2027
SEBI Regulation 16C	AI and machine learning used by SEBI-regulated entities	In force since early 2025, it places strict responsibility for AI outputs, data security and legal compliance directly on the regulated entity
RBI FREE-AI framework	AI used across banking and financial services	Published August 2025, it is currently advisory rather than binding, but signals the direction of future binding rules
CERT-In directives	All cybersecurity incidents, including AI-related breaches	Mandates rapid incident reporting, including notification within six hours of detection for regulated financial entities
EU AI Act	Any AI system serving EU-based users or customers	Applies extra-territorially to GCCs supporting EU-facing business units or clients

Regulatory penalties for weak AI governance are becoming severe enough to change board priorities on their own. Gartner predicts that through 2027, manual AI compliance processes will expose **75%** of regulated organizations to fines exceeding **5%** of global revenue, while more than **40%** of AI-related data breaches globally are expected to arise from cross-border misuse of generative AI by 2027.

3.3 Roadmap: Closing the Gap in 18 to 24 Months

Phased Roadmap : Closing the Gap in 18 to 24 Months



Phase	Timeframe	Key Workstreams	Success Metric
Phase 1: Stabilize	Months 1 to 6	Complete an AI asset inventory, close the highest-risk quick-win gaps, and stand up a formal AI governance charter with board sponsorship	**100% of production AI systems inventoried and risk-rated**
Phase 2: Integrate	Months 5 to 14	Deploy zero trust access controls for agents, build AI-specific monitoring and detection, and map every control to DPDP, SEBI, RBI, and CERT-In requirements	**Mean time to detect an AI-specific incident reduced by half**
Phase 3: Institutionalize	Months 12 to 24	Stand up a dedicated security center of excellence, run continuous red teaming against agents, and report AI risk metrics to the board on a recurring cadence	**GCC reaches Stage 4, Resilient by Design, on the maturity model**

Strategic Recommendations

- **Make AI Governance a Board-Level Mandate:** SEBI, RBI, and DPDP are putting direct accountability on boards for AI outcomes. For MNCs, this means parent board oversight of India GCC AI risk is nonnegotiable.
- **Action needs to be taken:** Establish a joint parent-GCC board-level AI risk committee with quarterly reporting.
- Fund AI Security as a Separate Line Item: US parent breach costs average $10.22M, and that liability flows back to your GCC. Shadow AI adds another $670K per breach. Gartner projects AI security will hit 40% of cybersecurity budgets by 2027.
- **Action needs to be taken:** Create a dedicated AI security budget with US breach cost exposure priced in.
- **Report AI Risk Like Financial Risk:** MNC boards expect financial-grade reporting. Use the four-stage maturity model as your shared scorecard across parent and GCC.
- **Action needs to be taken:** quarterly board reporting using the maturity model track DPDP, CERT-In, SEBI 16C, and RBI FREE-AI compliance.
- **Build 24-Hour Audit Readiness for Global Regulators:** DPDP, GDPR, and sectoral regulators all demand audit-ready documentation. MNCs face scrutiny from multiple jurisdictions simultaneously.
- **Action needs to be taken:** Maintain continuously updated, regulator-ready documentation, model cards, data provenance, and incident plans available within 24 hours.
- Inventory Every AI Asset—Including Shadow AI: MNCs are blocking all AI tools on client projects to protect proprietary code. Unsanctioned AI processing Indian personal data is a DPDP violation with global consequences.
- **Action needs to be taken:** complete 100% inventory and risk classification of all AI assets within 30 days.
- Put Agent Identity on Par with Human Identity: Treat AI agents as "privileged users that never sleep" with timebound access, segregated duties, and full logging. This mirrors the zero-trust mandates already in place for human identities in MNCs.
- **Action needs to be taken:** Implement just-in-time credentials and cryptographic verification for all agent-to-agent calls.
- Close Shadow AI with Technical Controls—Policy Alone Fails: Only 17% of organizations have technical controls to prevent sensitive data from reaching unapproved AI tools. MNCs are already discovering proprietary code in public AI training data.
- **Action needs to be taken:** Deploy DLP, content filtering, and sanctioned AI tooling with enterprise licenses within 90 days.
- Align Incident Response with CERT-In's 6-Hour Rule: CERT-In mandates reporting within six hours, faster than GDPR's 72 hours. MNCs must have playbooks that satisfy both Indian and home-country regulators.
- **Action needs to be taken:** Develop AI-specific incident response playbooks with documented 6-hour reporting capability and conduct quarterly tabletop exercises.
- Design Security In—Don't Bolt It On: Retrofitting security onto AI systems after deployment is expensive and structurally insufficient. MNCs must mandate security-by-design across all GCC AI development.
- **Action needs to be taken:** Embed security architects in AI product teams from the first specification.
- Build One Unified Governance Program Across All Regulators: MNCs face DPDP, GDPR, SEBI 16C, RBI FREE-AI, and home-country regulations simultaneously. A single unified program prevents fragmented compliance and audit fatigue.
- **Action needs to be taken:** Establish a single governance program covering all regulatory frameworks—not separate efforts per regulator or geography.

Conclusion

AI has expanded the GCC attack surface faster than GCC security programs have adapted to defend it. A workforce that was hired and trained to secure applications, endpoints, and networks is now responsible for models that can be manipulated through the content they read, agents that can be tricked into misusing their own permissions, and multi-agent systems where a single injection can propagate like a virus across the enterprise.

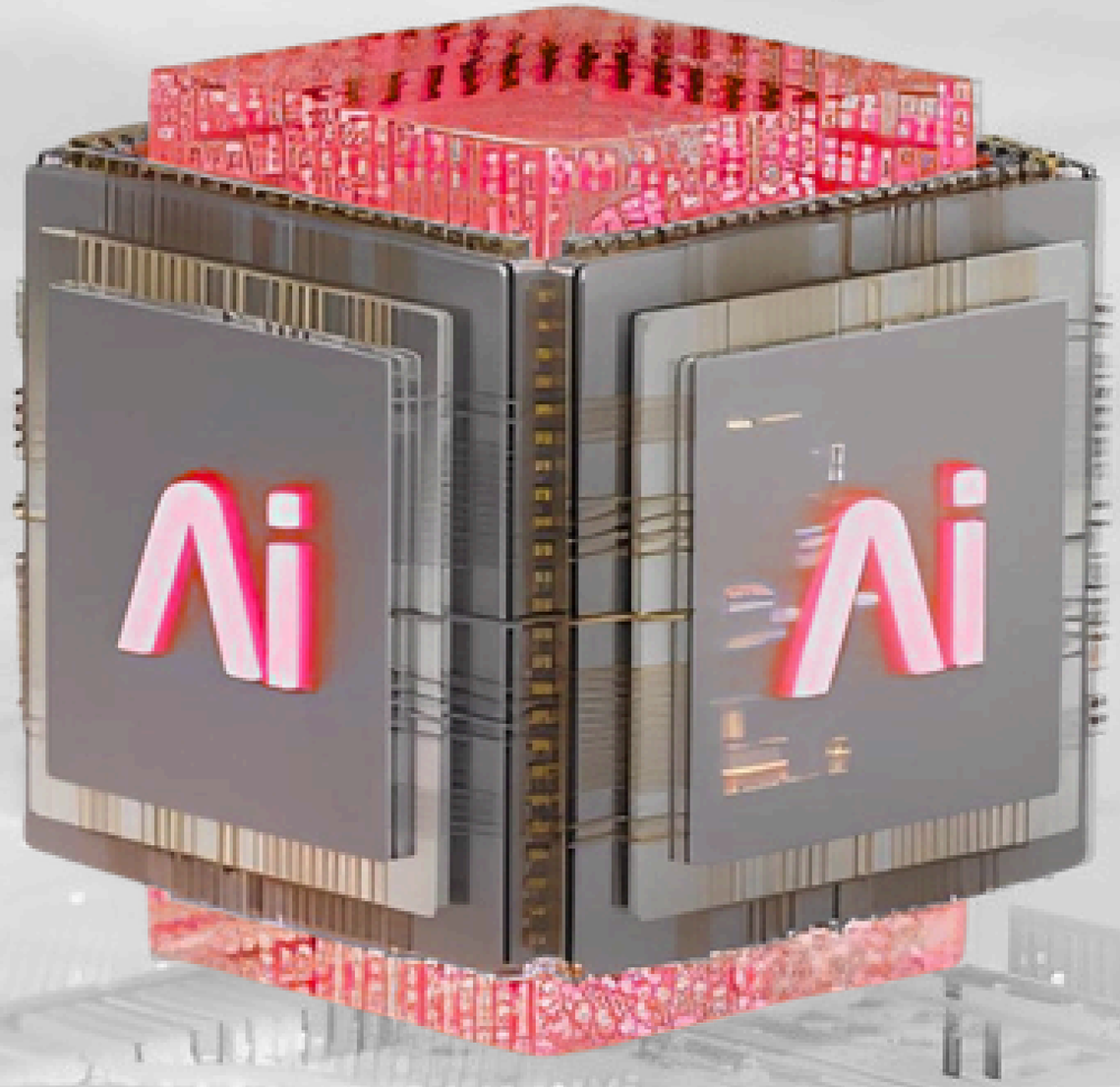
With nearly all tested AI agents vulnerable to prompt injection and inter-agent exploits, and fewer than half of GCCs operating advanced security frameworks, the gap between what is being built and what is being protected has become the defining risk of this decade for India's GCC/ODC sector.

> This gap is closeable, but not through incremental patching. The evidence in this report shows that the organizations absorbing the largest losses are overwhelmingly those without basic AI governance and access controls in place—meaning most of today's breach cost is structural, not inevitable.

The seven-layer security-by-design framework and four-stage maturity model set out here give GCC leaders a way to move deliberately from reactive, perimeter-only postures toward continuous, self-correcting resilience, rather than reacting to whichever regulator or incident forces the next round of investment.

The regulatory runway is also shortening. DPDP enforcement, SEBI Regulation 16C, RBI's FREE-AI framework, and CERT-In's six-hour reporting mandate are converging on the same expectation: boards, not just security teams, are accountable for AI outcomes. GCCs that treat security as a design input embedded in agent identity, data flows, and model deployment from day one will meet that bar as a matter of course.

Those that wait for the retrofit will pay. for it twice: once in breach cost and again in the compliance debt of catching up under scrutiny. The 18-to-24-month roadmap in this report is the difference between choosing that outcome and having it chosen for you.



References

- GCC/ODC Global Market Report, 2025.
- Industry Survey on GCC/ODC Generative AI and Agentic AI Adoption, 2025.
- Independent Benchmark Study, AI Agent Susceptibility to Manipulation, 2025.
- EY India, GCC Pulse Report 2025.
- OWASP, Top 10 for LLM Applications, 2025.
- Academic Red-Teaming Study, Black-Box Prompt Injection Technique, 2025.
- Academic Study, Tool Poisoning Technique Against Tool-Selecting Agents, 2025.
- Academic Study, Mixed Attack Strategy Across Model Backbones, 2025.
- Academic Study, Direct Injection Attacks Against Web Agents, 2026.
- Gravitee, State of AI Agent Security Survey, 2026.
- Darktrace, State of AI Cybersecurity 2026 Report.
- Dark Reading, Poll on Top Cybersecurity Attack Vectors, 2026.
- OWASP GenAI Security Project, State of Agentic AI Security and Governance v2.01, 2026.
- IBM Security and Ponemon Institute, Cost of a Data Breach Report 2025.
- Kiteworks, Research on Shadow AI and Data Governance Controls, 2025.
- Gartner, Survey on Deepfake and Generative AI Attack Prevalence, September 2025.
- Reporting on Arup (Hong Kong) Deepfake CFO Fraud Incident, February 2024.
- ISC2, 2025 Cybersecurity Workforce Study.
- Gartner, Security Spending Forecast, 2026.
- Gartner, Forecast on AI Compliance and Cross-Border Breach Risk Through 2027.
- Government of India, Digital Personal Data Protection (DPDP) Act, 2023.
- Securities and Exchange Board of India (SEBI), Regulation 16C.
- Reserve Bank of India (RBI), FREE-AI Framework, August 2025.
- Indian Computer Emergency Response Team (CERT-In), Cybersecurity Incident Reporting Directives.
- European Union, EU Artificial Intelligence Act.
- EY India / GCC Journal, GCC Cybersecurity Maturity Benchmarking Data, 2025–2026.

Inductus GCC Service Models

India's Leading GCC Enabler

BOT (Build-Operate-Transfer)

A structured pathway to establishing your GCC with minimized risk and maximum efficiency. We **build** and **operationalize** your center, ensuring seamless performance before **transferring full ownership** to you—**equipping your business with a mature, self-sustaining capability.**

COPO (Company-Owned, Partner-Operated)

Maintain **full ownership** while leveraging Inductus' operational expertise. This model enables you to establish a GCC with **absolute control over intellectual assets (IP), agility**, **and scalability** while we manage day-to-day operations, **ensuring zero liability, compliance, and maximum efficiency**.
Additionally, a **Zero Capex Model** with **Digital Twin or a Mirror Like Operational Structure** with superior process excellence.

FLEXI (Adaptive & Custom GCC Solutions)

Beyond predefined structures, **Flexi is a bespoke model offering absolute customization and adaptability.**

It molds itself around your unique business prerequisites, evolving seamlessly with your vision. **This isn't just a service—it's an agile, high-impact partnership crafted to maximize your success.**

OSDC (Offshore Service Delivery Center)

An Offshore Service Delivery Center (OSDC) provides a dedicated operational team managed by Inductus and aligned to the client's governance, technology, and business objectives. Unlike conventional outsourcing, teams are built exclusively for one enterprise with a structured approach to capability development, operational governance, and continuous improvement.

Proud recipient of **Times Power Icons Award** for being one of the **Leading GCC Enabler of India**

Presented by Bennett & Coleman THE TIMES OF INDIA

Inductus ensures that each model is executed with precision, innovation, and strategic foresight—helping you unlock the full potential of your GCC in India.

Our deep expertise in GCCs, coupled with a strong network of industry partnerships and policy-level advisory, positions us as a trusted partner for driving transformational outcomes.

Certificate of Excellence' for Consulting & Advisory Services by **Chicago Open University USA**

+91-92346-92346 gcc@inductusgroup.com www.indcutusgcc.com

COPO & Digital Twin Integrated Service Model

A study based proposition to build a global standard GCC mechanism for Large & Mid-sized Corporations

"In a world full of rapid tech & process disruptions, global corporations that invest in innovation-led R&D don't just survive—they lead. Innovation is the key to staying relevant, cost-competitive, and future-ready in an ever-evolving marketplace..."

Alouk Kumar - CEO, Inductus

Inductus GCC's Digital Twin and COPO (Company-Owned, Partner-Operated) Service Model creates a seamless, future-ready operational framework for global businesses setting up GCCs in India. The Digital Twin Process ensures real-time collaboration, decision-making, and operational efficiency by replicating physical systems in a virtual environment, enabling synchronized execution across multiple time zones. Meanwhile, the COPO Model allows MNCs to retain full ownership and strategic control while leveraging Inductus' expertise for execution, compliance, and scalability.

This hybrid approach optimizes costs, mitigates risks, and accelerates GCC growth, ensuring innovation-driven operations with minimal liabilities and maximum efficiency.

Built in India.
Designed for the World.

www.inductusgcc.com