VERTARA global
GCC ADVISORY

NANO GCC SERIES · PAPER 4

Nano GCCs as a Risk Management Strategy

Why the risks a nano GCC removes, and the risks it adds, belong on the board agenda

Thought leadership · 5–7 minute read

In brief. A nano GCC (a 20–200 person capability centre) can reduce a mid-market company's exposure to vendor concentration, AI talent scarcity and geopolitical shocks. But a small centre also carries its own risks: key people, thin benches, compliance gaps and governance drift. Its value as a hedge depends on assessing and managing both sides from day one. This paper sets out the risks a nano GCC can offset, the risks it brings, a board-level scorecard and the controls that matter at each stage.

Why risk belongs in the GCC conversation

Most GCC business cases are built on cost and capability. Risk usually appears as a single line on the last slide. That is a missed opportunity, and a blind spot.

The missed opportunity: owning a small, well-run capability centre gives a company something it cannot buy from a vendor, which is control. Control over who does critical work, where it is done, and how quickly it can be moved or scaled.

The blind spot: a small centre carries risks of its own. One resignation, one failed audit or one disengaged sponsor at headquarters can undo it.

> **"A 50-person centre is not a smaller version of a 5,000-person one. It is more fragile."**

India's GCC base now stands at 2,117 centres, employing about 2.36 million people (Nasscom-Zinnov, FY26). As more mid-market firms join that count with small centres, the question for boards shifts. It is no longer *should we have a GCC?* It is *what risks does it remove, what risks does it add, and who is managing both?*

The enterprise risks a nano GCC can offset

A nano GCC works as a hedge when it moves critical capability from *rented* to *owned*. Four exposures stand out.

1. Vendor concentration. Many mid-market firms run engineering, data or operations through one or two large service providers. That keeps procurement simple, but it concentrates knowledge, pricing power and exit difficulty in someone else's hands. The July 2024 CrowdStrike incident, where one faulty update affected about 8.5 million Windows devices, showed how a single supplier can become a single point of failure. Regulators have noticed. The EU's DORA, applicable since January 2025, requires financial entities to assess ICT concentration risk

before contracting and to hold exit strategies. A small owned team that holds the architecture, the code and the know-how is a practical exit strategy.

2. Dependency on large providers' priorities. For a top-tier vendor, a mid-market account is rarely the priority. The best people rotate to bigger clients, and roadmaps follow the vendor's portfolio rather than yours. A nano GCC lets a company keep its most differentiated work in-house and buy only commodity work from vendors.

3. AI and specialist talent scarcity. ManpowerGroup's 2026 survey of 39,000 employers found 72% struggle to fill roles, with AI skills now the hardest to find. In India, TeamLease Digital estimates the GenAI skills gap at about 53%. Companies that rely on a vendor's bench get whoever is free. Companies with their own centre can recruit, train and retain a small core of the people they actually need.

4. Geopolitical and policy fragmentation. Visa, immigration and cross-border employment policies continue to shift across major markets, creating uncertainty for firms that rely heavily on moving talent across borders. A company that can do the work where the talent already is, rather than moving people to the work, has more room to adapt. A presence in more than one country adds a further layer of optionality.

For PE-backed businesses, the case is sharper still. Nano GCCs can reduce dependency on incumbent service providers, preserve institutional knowledge during ownership transitions, and make the business more attractive to future buyers, who increasingly look at who actually owns critical capability.

A note of caution: *a GCC is not a shield against every policy change. Some proposed measures, such as the US HIRE Act, would reach payments to foreign affiliates as well as vendors. Operating model choices should be stress-tested against tax and policy scenarios, not assumed to be immune.*

Resilience: faster recovery, not immunity

A nano GCC cannot prevent outages, but it can improve recovery by ensuring architectural knowledge and decision rights remain inside the enterprise. When a supplier fails, as in the CrowdStrike incident, the companies that recover fastest are those that understand their own systems and can act without waiting in a vendor's queue. Three things matter:

- **Business continuity:** critical processes have an owner inside the company and a documented fallback.
- **Disaster recovery:** recovery runbooks are held and rehearsed in-house, not only in a vendor's playbook.
- **Critical knowledge ownership:** architecture, integrations and key code are understood by the company's own people, so decisions in a crisis do not depend on a third party.

The risks a nano GCC brings with it

> **Nano GCCs do not eliminate risk. They redistribute it.** The question for the board is whether the risks taken on are smaller, and better controlled, than the risks given up.

Small centres fail differently from large ones. In a 3,000-person centre, a few exits are absorbed. In a 40-person centre, the same exits can stall a product line. These are the risks we see most often in practice.

Risk	Why it bites harder at nano scale	Early warning sign
Key-person dependency	One or two people hold the architecture, the client context or the site leadership	Work routes through the same names; no documented succession
Attrition	Each exit is a large share of capacity and knowledge	Rising offers from larger GCCs nearby; flat career paths

Risk	Why it bites harder at nano scale	Early warning sign
Thin leadership bench	The site leader is also hiring manager, HR partner and finance contact	Leader time spent on admin rather than delivery
Compliance and entity gaps	Small teams rarely have in-house legal, tax or payroll depth	Late filings, unreviewed transfer pricing, unclear data-handling rules
Headquarters sponsorship	A centre this size depends on one or two executive champions	Sponsor changes role; GCC drops off the leadership agenda
Governance drift	Informal decisions that worked at 20 people stop working at 120	No operating rhythm, no scorecard, escalations by email
Location concentration	Choosing a hot market means competing with many larger centres for the same talent	Offer declines and counter-offers rising

The last point deserves emphasis. Two-thirds of new GCCs in India choose Bengaluru or Hyderabad (Nasscom-Zinnov). A nano GCC that diversifies vendor risk but then competes head-on with many larger employers for the same engineers may simply have swapped one concentration for another.

And there is year two. Many GCCs perform well in the set-up phase, when attention is high, and then struggle once the launch team moves on. For a nano centre, that dip can be terminal. This is often where external support remains valuable, as many nano GCCs face their greatest sustainability challenges after the initial launch phase.

A risk scorecard for the board

A board does not need a 60-tab risk register. It needs a short scorecard that answers two questions together: *how exposed are we today?* and *does our GCC reduce that exposure or add to it?* We suggest scoring each dimension red, amber or green, before set-up and every six months after.

Dimension	What to measure	Red flag
Vendor concentration	Share of critical capability delivered by the largest provider; time and cost to switch	One provider holds core IP or knowledge with no tested exit plan
Capability ownership	Which critical roles, code and decisions sit in-house versus with vendors	The GCC does only work a vendor could take back tomorrow
Talent resilience	Attrition, offer-acceptance rate, depth behind each critical role	Any critical role with no trained backup
Location and policy exposure	Share of capacity in one city or country; sensitivity to visa, tax and data rules	All capacity in one market with no contingency site or partner
Compliance and entity health	Filings, transfer pricing, data protection, employment law, audit findings	Overdue filings or unreviewed intercompany pricing
Governance and sponsorship	Named executive sponsor, operating rhythm, scorecard reviewed at leadership level	Sponsor gap or no formal review in the last two quarters
Value delivered	Outcomes against the business case, not just headcount	Growth in seats with no change in ownership of critical work

Five questions every board should ask

1. If our largest service provider failed or walked away, how long before critical work stops?
2. Which three people in our GCC would we least like to lose, and who is behind them?

3. What would we do if a visa, tax or data rule changed in our main delivery country next quarter?
4. Who at headquarters owns the GCC's success, and what happens if they move on?
5. Is the GCC taking on more critical work each year, or just more volume?

Managing the risks across the lifecycle

Risk management for a nano GCC is not a one-off assessment. The controls that matter change as the centre moves from design to steady state.

1 · Design	2 · Set up	3 · Year 1	4 · Year 2 and beyond
▸ Baseline the scorecard	▸ Entity, tax, payroll	▸ Document know-how	▸ Scorecard every 6 months
▸ Map critical roles	▸ Data and IP controls	▸ Backup for each role	▸ Build leadership bench
▸ Stress-test location	▸ Hire leaders early	▸ Monthly ops review	▸ Own more critical work
▸ Name the sponsor	▸ Vendor exit plan	▸ Career paths, retention	▸ Option: second site

Year 2 is where nano GCCs most often slip, after the launch team moves on.

Early controls are about getting the foundations right: the entity, the location and the first leaders. Later ones are about resilience: making sure no single person, sponsor or site can take the centre down.

The multi-country nano hub option. Some companies take the hedge one step further, running two or three small hubs in different countries rather than one larger centre. This spreads location, policy and talent risk, and allows work to move if one market tightens. But each hub needs its own entity, compliance, leadership and culture, and coordination costs rise with every site. We generally advise proving one hub through year two before adding a second, and adding it for a specific risk reason rather than for symmetry.

When a nano GCC is not the right hedge

A GCC is one risk tool among several. It is the wrong one when:

- **The work is genuinely commodity.** If any capable vendor could do it and switching is easy, concentration risk is low, so a multi-vendor contract may be cheaper and simpler.
- **There is no committed sponsor.** Without an executive who owns the outcome, the centre will drift, and an orphaned GCC is a risk in itself.
- **The company cannot fund year two.** A centre set up on a one-year budget, with no plan for leadership, career paths and compliance, is likely to struggle just as it should start paying back.
- **The real problem is elsewhere.** Weak product strategy or unclear decision rights at headquarters will not be fixed by moving work offshore.

In these cases, better vendor contracts, a second supplier or a hybrid or partner-operated model may give more protection for less effort. The right operating model depends on the risk being managed.

What boards should take away

- **Treat the GCC as a risk decision as well as a cost decision.** Put vendor, talent and policy exposure into the business case, not just the savings.
- **Assess both ledgers.** Score the risks the centre removes and the risks it adds, before set-up and every six months after.
- **Make the controls proportionate.** A nano GCC does not need big-company bureaucracy. It does need succession cover, clean compliance and a named sponsor.

- **Plan for year two on day one.** The launch is the easy part. Resilience is earned in the second and third years.

How Vertara helps

Vertara Global is a practitioner-led GCC advisory firm working with mid-market companies across sectors. We help clients run the risk assessment before committing, choose the operating model that fits the risk they are managing, set up the entity, talent and governance controls, and stay engaged after handover to keep the centre on track. Every engagement is led by a senior practitioner.

Sources

- Nasscom-Zinnov, GCC Landscape in India 2026 (report PDF)
- Business Today: India's GCC story hits 2030 target four years early
- TechCrunch: Microsoft says 8.5M Windows devices affected by CrowdStrike outage
- IBA: DORA and digital operational resilience
- ManpowerGroup: 2026 Global Talent Shortage
- YourStory: TeamLease Digital on GenAI and cloud talent gaps
- RSM: HIRE Act proposes 25% excise tax on outsourcing

© 2026 Vertara Global. This paper is for general information and does not constitute legal, tax or investment advice.