NANO GCC REAL ESTATE · POINT OF VIEW

A Small Team Needs Enterprise-Grade Resilience

A nano GCC may seat 25 people, but the work it runs can matter to the whole group. Why workplace controls should follow the consequence of an outage, not the headcount, and how to size them before you sign.

Vertara Global · Point of View · October 2026

AT A GLANCE

- A nano GCC (20 to 200 people) often runs a large share of one global process, so a small outage can become a group-level incident.
- The disruptions are ordinary and local: water, air quality, power and connectivity, plus incident-reporting clocks that start within hours[1],[2].
- Classify the work by how long it can stop, verify each control with evidence, and rehearse the fallback before launch.

01 The trap

A company sets up a 25-person finance centre in Pune. The team runs month-end reconciliation for a group operating in a dozen countries. The office was chosen the way most small offices are: on rent, fit-out and commute, in a good building with a generator and a reputable landlord. On the second day of close, roadworks cut the building's only fibre route. The generator runs; the network does not. Laptops are set up for the office network only, the flex centre named as the alternate site has never been booked, and the one person who knows the carrier's escalation path is on leave. The team is back online by evening. The close slips by a day.

The cause is rarely a bad building. It is a workplace specified by headcount. A nano GCC has a concentrated risk profile: few people, but often a large share of one process, and no spare floor to move to. Measured in desks, the outage was minor. Measured in consequence, it delayed group reporting. The controls a site needs should follow what happens when the work stops, not how many people do it.

> *Enterprise-grade does not mean enterprise-sized. It means the right few controls, verified, owned and rehearsed before the first day of operations.*

02 Why the risk is sharper in 2026

In CBRE's 2026 India occupier survey, about half of respondents named poor air quality as a major infrastructure threat, 31% flagged water availability and quality, and 29% said waste and sanitation problems could affect productivity[3]. These are not abstractions. During Bengaluru's water shortage in March 2024, several companies

[1] CBRE, India Office Occupier Survey 2026, press release on commute and workplace infrastructure (September 2026). www.cbre.co.in/press-releases/70-firms-see-commute-as-most-crucial-consideration

[2] Trilegal, "2022 CERT-In directions on reporting cyber incidents" (directions dated 28 April 2022). trilegal.com/knowledge-repository/2022-cert-in-directions-on-reporting-cyber-incidents

[3] CBRE, see note 1.

let staff work from home because employees could not or would not come in[4]. In Delhi-NCR, the November 2025 revision of the Graded Response Action Plan lets state governments cap public and private offices at 50% strength from Stage III[5]. And India's peak power demand hit a record 256.1 GW on 25 April 2026[6].

Facilities built for uptime are not immune. Uptime Institute's 2026 outage analysis found power is still the leading cause of impactful outages, connectivity failures are rising and tend to last longer, and not following procedures remains the main driver of human-error outages. 57% of respondents said their latest major outage cost more than $100,000[7].

These are different data series, some covering data centres rather than offices, and none of them predicts how a particular building will perform. Together, though, they point one way: assume the site will be disrupted, and decide in advance what the team does when it is.

03 Looking ahead: 2027 and beyond

Three shifts will raise the bar for small centres:

- **Regulatory clocks become real.** CERT-In's 2022 directions already require cyber incidents to be reported within six hours of being noticed[8]. Under the DPDP Rules, notified in November 2025, breach notification to the Data Protection Board applies from May 2027, with a detailed report due within 72 hours[9]. The clock runs the same for 25 people as for 2,500, so an incident lead, a contact tree and an evidence trail need to exist on day one.
- **Disruption becomes seasonal, not exceptional.** Air-quality curbs in the north and water stress in the south recur most years. A work-from-home fallback that has never been run at full strength is a hope, not a plan.
- **The fallback may be in another city.** Colliers expects the next phase of GCC growth to come partly from smaller formats and expansion into Tier II and III cities[10]. For a growing nano GCC, a planned second site can double as a recovery location, if systems and access are set up for it from the start.

04 Three rules for a resilient small site

Classify the work before you choose the building. List what the team does on site and how long each activity can stop before it hurts. Put the business, IT, security and HSE owners in the same room; each sees a different risk. Most nano GCCs land in three tiers (section 06), and one centre can hold all three.

Verify every control; don't assume it. Ask the landlord or operator for evidence, not assurances: what the generator actually powers, which carriers enter the building and by which routes, how long access logs are kept, the fire NOC and the date of the last drill, water storage and supply contracts. Record everything the team relies on but does not control. Those dependencies are where small sites get caught out.

Rehearse the fallback before launch. Write down who declares an incident, who calls the vendors, and who tells employees and the global process owner. Then run a one-hour tabletop: the building loses power at 10 am on

[4] PTI, as reported in "Water crisis in Silicon Valley of India presents pressing challenge, say industry players" (Outlook Business, 17 March 2024). www.outlookbusiness.com/news/water-crisis-in-silicon-valley-of-india-presents-pressing-challenge-say-industry-players

[5] CAQM revision of GRAP, as reported in "Delhi air pollution: public and private offices can work at 50 per cent strength under GRAP III after revision" (The Week, 22 November 2025). www.theweek.in/news/india/2025/11/22/delhi-air-pollution-work-from-home-and-public-private-offices-to-work-at-50-per-cent-strength-during-grap-iii

[6] "India records all-time high peak power demand of 256.1 GW, meets supply without shortage" (SolarQuarter, 29 April 2026). solarquarter.com/2026/04/29/india-records-all-time-high-peak-power-demand-of-256-1-gw-meets-supply-without-shortage

[7] Uptime Institute, Annual Outage Analysis 2026, as reported in "Uptime announces Annual Outage Analysis Report 2026" (ITWeb Africa, May 2026). itweb.africa/article/uptime-announces-annual-outage-analysis-report-2026

[8] Trilegal, see note 2.

[9] AZB & Partners, "Update: India's Digital Personal Data Protection framework comes into effect" (19 November 2025). www.azbpartners.com/bank/update-indias-digital-personal-data-protection-framework-comes-into-effect

[10] Colliers, as reported in "GCC leasing to reach 40 million sq ft by 2027" (Construction World, 25 July 2026). www.constructionworld.in/latest-construction-news/real-estate-news/gcc-leasing-to-reach-40-million-sq-ft-by-2027--colliers/95000

close day. It is the cheapest test there is, and it nearly always finds something: an old phone list, laptops that cannot reach a system off-network, an alternate site nobody has keys to.

05 What resilience is worth

Return to the opening scenario. Option A uses the building as it is: one carrier, landlord backup power and an untested work-from-home plan, so a disruption costs about eight hours. Option B adds a second carrier on a separate route, backup power for IT, pre-configured remote access and a standby flex arrangement for ₹1.2 lakh a month, and the team is working again within about an hour. We costed staff time at ₹1,500 an hour and ran three kinds of year.

EXHIBIT 1 · ONE-YEAR COST OF DISRUPTION (ILLUSTRATIVE)

Year	Disruptions	Option A	Option B	A minus B
Quiet	One, off-deadline	₹3.0 lakh	₹14.8 lakh	−₹11.8 lakh
Typical	Three, off-deadline	₹9.0 lakh	₹15.5 lakh	−₹6.5 lakh
Bad	Three, one on close day	₹59.0 lakh	₹15.5 lakh	+₹43.5 lakh

Assumptions chosen for clarity, not market quotes. Each disruption lasts eight hours under Option A and one hour under Option B. Option B includes ₹14.4 lakh a year of added cost. The bad year assumes a missed close costs ₹50 lakh in overtime, audit and customer impact. 25-person team. Vertara Global analysis.

On staff time alone, Option A wins every year, by ₹6.5 to ₹11.8 lakh: that is the price of the insurance. One disruption on the wrong day reverses the result by ₹43.5 lakh. In a typical year, Option B pays for itself if a single missed deadline costs more than about ₹6.5 lakh. Price resilience against the process, not the payroll.

06 How to run the decision

Make the resilience standard part of site selection, not a fit-out afterthought. Start by agreeing the tier of each activity the centre will run.

Tier	What the site needs	Decision test
Critical: can pause for hours	Two carriers on separate routes; backup power for IT and essential cooling; tested remote access or a standby site; a named incident lead every shift	Can the team be working again within an hour, on the worst day of the month?
Important: can pause for about a day	A resilient primary link plus mobile backup; UPS for an orderly shutdown; a written work-from-home fallback with system access checked	Has the fallback been run at full team strength, not just on paper?
Routine: can pause for several days	Standard building services; a current contact list; a clear owner for the work-from-home call	Does everyone know who makes the call, and how they will hear it?

Illustrative tiers. Set the thresholds with the business process owner, not the facilities team alone.

- **Write a one-page standard.** For each tier, set minimum power, network, access, safety and incident-response requirements, and agree them with IT, security and HSE before shortlisting sites.
- **Score sites on evidence.** Compare shortlisted buildings on one schedule. Mark every control that depends on the landlord or operator, and check what the lease or service agreement actually commits them to.

- **Assign owners and dates.** Facilities owns building services; IT owns network and remote access; security owns access and incident response; HR owns employee communication; the business owns the decision to switch to the fallback.
- **Test before go-live, then on a cycle.** Run the tabletop before the first day of operations, and again whenever a new function joins the centre.
- **Re-tier as the mandate grows.** A centre that takes on a customer-facing or regulated process moves up a tier, and the site standard should move with it.

QUESTIONS FOR THE BOARD

1. Which activities in this centre cannot pause for a day, and who signed off on that?
2. Which controls do we own, and which depend on the landlord or operator?
3. When was the fallback last tested, and what broke?
4. Which regulatory clocks start if this site has an incident, and who starts them?

07 How Vertara Global helps

We start with the work, not the floor plan. Before a site is shortlisted, we classify the processes the centre will run and agree a resilience standard with the client's IT, security and HSE owners. Site due diligence then looks for evidence, records every dependency on the landlord or operator, and feeds the lease negotiation so the critical obligations are written down, not promised.

Whichever operating model the client chooses, we run the first recovery exercise with the team and hand over an operating pack: site risk register, service dependencies, emergency contacts and recovery procedures, each with a named owner. We stay engaged into year two, re-tiering controls as the mandate grows. The test of success: a disruption that costs the team an hour, not the group a deadline.

ABOUT VERTARA global

Vertara Global is a practitioner-led GCC advisory firm. We help mid-market companies across sectors and geographies design, set up, scale and transform their Global Capability Centres, from the first business case and location choice to the operating model, entity, talent and workplace.

Our services span five pillars:

1. **GCC Consulting**
2. **Legal & Entity Support**
3. **People Advisory**
4. **Digital & AI**
5. **Engineering GCC Solutions**

Client-first and leader-led: senior practitioners run every engagement, and we stay involved after handover, because year two is where many GCCs are tested.