PROACTIVE™
Enhancing Digital Experience

GCC India Infrastructure Setup Guide: Network, Collaboration, Security, and Identity for the CIO of a New or Growing India Centre.

The specific network topology from Bengaluru or Hyderabad to Frankfurt, London, or New York. The collaboration architecture that parent executives will judge in the first ninety days. The security operating model that inherits CERT-In and DPDP obligations from Day 1. What it actually costs. What actually breaks.

Written for the global CIO who has been handed technology charge of an India GCC, regardless of whether the entity is a WOS, a BOT, or a GCC-as-a-Service arrangement.

Version 1.1 · Updated August 2026 ·

Reflects DPDP Rules notified 13 November 2025, CERT-In Directions 28 April 2022, current AWS / Azure / GCP India regions, current Cisco Catalyst SD-WAN, Webex Suite, Room Series, and Industrial Threat Defense architectures, and current India telecom operator ILL and cloud on-ramp footprint.

Written by ***Deepak Sampath, Regional Manager (South)***

Proactive Data Systems GCC Practice

Cisco Preferred Partner across Networking, Security, Collaboration, Data Center, and Services · Cisco Advanced Customer Experience Specialised · Since 1991.

Preface

Every global CIO handed technology charge of an India GCC reads the same set of documents in the first month. The corporate secretary sends the entity-structuring paper. The CHRO sends the site-head brief. Real estate advisors send the location comparison. Big-four consultancies send the tax slide deck.

None of those documents answers the technology question. Where does the ILL land in Whitefield in Bengaluru versus Hitec City in Hyderabad, and which operator pair actually survives a monsoon? What is the round-trip latency from Bengaluru to your Frankfurt data centre when Airtel's Mumbai peering flaps, and which application in your parent stack will break first? Which Cisco Room Kit or Microsoft Teams Rooms configuration passes the test of a CFO joining a conference-room call three time zones out and hearing every voice clearly? What does your parent SOC need from Day 1 to see the India entity's endpoints alongside the rest of the estate, and what does CERT-In require the moment the entity is incorporated?

This guide answers those questions. It is deliberately narrow: it covers network, collaboration, security, and identity for a new or growing India GCC. It does not cover entity choice, location advisory, tax structuring, real-estate fit-out, HR, or executive sponsorship. Other firms cover that ground; we are not one of them. What we do is build and run the infrastructure that the entity, whichever way it is set up, actually needs on Day 1 and through hire waves 2, 3, and 4.

It is written by the Proactive Data Systems GCC Practice from live GCC infrastructure engagements with global parents across Europe, North America, APAC, and the Middle East. It is opinionated where the market rewards a clear position and honest about failure modes we have watched play out in real Indian centres. Consult your India systems integrator before acting on any specific technology decision.

Key Terms

ILL (Internet Leased Line)

Dedicated symmetric internet connectivity from an Indian telecom operator, standard for GCC underlays. Different from broadband; carries an SLA, static IP, and typically fibre-to-premises.

SD-WAN

Software-defined WAN overlay providing application-aware policy routing across mixed underlays (ILL, MPLS, LTE/5G). Cisco Catalyst SD-WAN is one of several parent-standard choices.

SASE

Secure Access Service Edge, a converged network and security architecture combining SD-WAN with cloud-delivered security. Most parents run a SASE fabric (Zscaler, Netskope, Palo Alto Prisma Access, Cisco+ Secure Connect with Umbrella) that the GCC connects into.

ZTNA

Zero Trust Network Access, session-level authenticated access to parent-private applications, replacing legacy full-tunnel VPN.

Cloud on-ramp

Direct interconnect from an ILL provider to a cloud region (AWS Direct Connect, Azure ExpressRoute, GCP Cloud Interconnect) in an Indian Data Center.

DPDP Act 2023

India’s Digital Personal Data Protection Act. Rules notified 13 November 2025. Applies to any entity processing personal data, including employee data of the GCC itself.

CERT-In Directions of 28 April 2022

Applies to every Indian entity. Six-hour incident notification, 180-day log retention within India, mandatory NTP synchronisation to NIC or NPL time sources.

SIEM / XDR

Security Information and Event Management / Extended Detection and Response, parent-side platforms into which the GCC's telemetry ingests. Common: Microsoft Sentinel, Splunk, IBM QRadar, Google Chronicle, Sumo Logic, CrowdStrike Falcon, SentinelOne, Cisco XDR.

In Brief

What Proactive Delivers for GCC Infrastructure:

Network architecture from India to parent HQ with dual-underlay ILL from independent Indian operators, Cisco Catalyst SD-WAN or parent-standard SD-WAN, direct interconnect to AWS Mumbai and Hyderabad, Azure Central India (Pune) and South India (Chennai) and West India (Mumbai), GCP Mumbai and Delhi. Integration with parent SASE fabric - Zscaler, Netskope, Palo Alto Prisma Access, or Cisco+ Secure Connect with Umbrella. Hybrid meeting rooms on Cisco Room Kit series, Microsoft Teams Rooms certified devices, or Zoom Rooms - matched to parent standard.

Collaboration platform build-out on Cisco Webex Suite, Microsoft Teams, or Zoom Workplace. Identity federation via Microsoft Entra ID, Okta, or Ping with MFA through Cisco Duo. Endpoint deployment with Windows, macOS, and Linux images and EDR (Cisco Secure Endpoint, CrowdStrike, SentinelOne, or Microsoft Defender for Endpoint). MDM via Microsoft Intune, Jamf, or Kandji. SIEM feed to parent SOC with a parallel India-view for CERT-In and DPDP. Day 1 CERT-In compliance and DPDP-aware data-flow design. Ongoing managed services option post-Go-Live. Costed to Indian market bands. The Proactive GCC India Infrastructure Setup Guide is available as a free download.

Who this is for:

Global CIOs, CTOs, and Heads of Infrastructure with technology charge of an India GCC, whether the entity was set up as a Wholly Owned Subsidiary, via Build-Operate-Transfer, or as a GCC-as-a-Service arrangement. India GCC Heads of IT are accountable for infrastructure operations from Day 1 through steady state.

Since:

1991. Proactive Data Systems is a Cisco Preferred Partner across five portfolios and Cisco Advanced Customer Experience Specialised.

What Does the GCC Infrastructure Stack Actually Look Like?

A modern GCC infrastructure stack has six layers, and every one of them is a Day 1 problem: network to parent and to cloud, campus LAN and Wi-Fi inside the office, collaboration for the parent-GCC hybrid, identity and access federated with parent, endpoint and MDM standardised to the parent build, and security integrated into the parent SOC while independently satisfying Indian regulatory obligations.

The stack in Cisco-standard reference form, with the parent-vendor variants Indian GCCs actually run:

Layer	Cisco-standard reference	Parent-vendor variants seen in Indian GCCs
WAN to parent and cloud	Cisco Catalyst SD-WAN + Cisco+ Secure Connect (SASE)	Zscaler ZIA/ZPA, Netskope, Palo Alto Prisma Access, Fortinet Secure SD-WAN, VMware VeloCloud
Campus LAN	Cisco Catalyst 9300/9500 switching	Aruba CX / Meraki (typically only where parent standardises)
Campus Wi-Fi	Cisco Catalyst 9166I (Wi-Fi 6E) or Wi-Fi 7 (9172/9176/9178/9179)	Meraki MR57, Aruba AP series
Collaboration platform	Cisco Webex Suite + Control Hub	Microsoft Teams (M365), Zoom Workplace
Meeting rooms	Cisco Room Kit series, Room Bar, Board	Microsoft Teams Rooms certified (Poly, Logitech, Yealink, Neat, Cisco), Zoom Rooms certified
Identity	Cisco Duo + parent IdP federation	Microsoft Entra ID, Okta, Ping Identity
Endpoint EDR	Cisco Secure Endpoint	CrowdStrike Falcon, SentinelOne Singularity, Microsoft Defender for Endpoint
MDM	(parent choice)	Microsoft Intune, Jamf, Kandji
Security telemetry	Cisco XDR	Microsoft Sentinel, Splunk, IBM QRadar, Google Chronicle, Sumo Logic

Two operating principles determine whether the stack works or fails:

- **Parent standardisation over local optimisation.** The GCC runs the same collaboration platform, endpoint EDR, and identity provider as the parent. Every place we depart from the parent standard, we create a support burden that outlives the setup team by years. Depart only where India-specific regulation forces it (SIEM tap for CERT-In visibility, MDM policies for local DPDP compliance), not for licensing savings.

- **India regulatory sovereignty.** The GCC entity is subject to Indian law regardless of parent domicile. CERT-In obligations start on incorporation. DPDP obligations start when the entity processes personal data, which for employee data is Day 1. The infrastructure must satisfy Indian regulators independently of what the parent SOC sees.

How Do You Engineer the Network from GCC to Parent HQ?

GCC-to-parent network engineering is three problems solved together: underlay reliability across Indian telecom paths that are less predictable than most parent CIOs assume; overlay architecture that policy-routes traffic to parent-private applications, SaaS, and India-market internet through the right paths; and cloud interconnect that removes the internet from the parent-to-India-cloud data path.

Dual-underlay ILL from independent operators. A Every India GCC runs two symmetric ILLs, typically 500 Mbps to 1 Gbps each in a 200-seat office, from separate operators. The operator pairings we have seen survive real Indian conditions best are Airtel + Tata Communications and Jio + Airtel. Vodafone-Idea + one of the above works in specific micro-markets. Different physical paths to the premises are non-negotiable; a single conduit cut in Bengaluru's Outer Ring Road takes both providers down if they share the last-mile duct, which happens more often than either operator will admit until you have watched it happen.

Operator diversity is non-negotiable, and pair selection is engagement-specific.
Every India GCC runs two symmetric ILLs from separate operators, with different last-mile paths to the premises; a single conduit cut in a Bengaluru or Hyderabad micro-market can take both providers down if they share the last-mile duct, which happens more often than either operator will document until you have watched it happen.

The four major Indian operators (Airtel, Tata Communications, Jio, Vodafone-Idea) each have distinct strengths across international transit paths, India-domestic performance, enterprise service maturity, and pricing at specific PoPs, and those strengths shift quarter on quarter as capacity, peering, and cable-system arrangements change. Match the operator pair to the parent-region path that matters most, validate with a real proof of concept before the lease commits, and do not pick a pair from habit or a corporate-standard list built for a different geography. On every engagement, we run the operator selection and validation against the parent's specific target regions before we specify the SD-WAN edge.

SD-WAN overlay policy-routing. Cisco Catalyst SD-WAN or parent-standard SD-WAN steers traffic to three distinct destinations: parent-private applications go via the parent's SASE fabric with ZTNA replacing full-tunnel VPN; SaaS (M365, Google Workspace, Slack, GitHub, Atlassian) egresses direct to the internet through the SASE security inspection; India-market internet uses local egress. Do not tunnel India-market traffic to a US or European PoP just because the SASE architecture makes it easy; the added latency degrades Indian government portals, local banking, and Aadhaar-authenticated services.

Cloud on-ramp. Where the parent or GCC runs cloud workloads in AWS Mumbai (ap-south-1) or Hyderabad (ap-south-2), Azure Central India (Pune) / South India (Chennai) / West India (Mumbai), or GCP Mumbai (asia-south1) and Delhi (asia-south2), direct interconnect via AWS Direct Connect, Azure ExpressRoute, or GCP Cloud Interconnect delivers 10-30% lower latency than internet egress, predictable throughput, and typically 30-50% lower egress cost at scale. In practice, we terminate customer cross-connects in NTT-Netmagic, Sify, CtrlS, or STT GDC data centres in Mumbai and Hyderabad, depending on where the parent's cloud footprint lives.

MPLS: where and why. Some parents retain MPLS for latency-sensitive or regulatory paths (trading systems, real-time financial-services applications, some SAP-to-SAP paths). Design the GCC to accept MPLS where the parent requires it. Do not lead with it: modern SD-WAN over dual-ILL matches or beats MPLS for cost and flexibility in every GCC use case we have delivered in the last four years.

What Is the Real Latency and Failure-Mode Reality on India-to-Parent Paths?

Round-trip latency and jitter to parent HQ shape which applications work well from the GCC, which need architectural rework, and which need India-local instances. The numbers below are typical Indian ILL-over-tier-1-transit measurements from Bengaluru or Hyderabad to major parent geographies, real numbers we see in production, not marketing figures.

Parent geography	Typical RTT (ms)	Practical impact
Singapore, Hong Kong	60-90	Excellent. Most applications work as if local
Tokyo, Seoul, Sydney	100-140	Very good. Voice, video, and most database work fine
Dubai, Frankfurt, Amsterdam	130-170	Good. Well-designed applications work; chatty protocols degrade
London, Zurich, Paris	140-180	Same as above
US East (Virginia, New York, Boston)	190-230	Marginal for chatty protocols; asynchronous work is essential
US Midwest (Chicago, Dallas)	210-250	Marginal; expect architectural work
US West (California, Seattle)	230-260	Difficult for interactive traffic; India-local instances often required
Sao Paulo, Buenos Aires	300+	Very difficult; India-local instances required for most workloads

What actually breaks. Chatty database protocols (SQL Server client-server, legacy Oracle applications, older Windows file shares over SMB), CAD/EDA tools that were designed for a LAN environment (specific SolidWorks, ANSYS, Cadence, and Synopsys workflows), specific ERP client-server modes, and older Citrix or RDP topologies where the display protocol was tuned for a metro-area network. Modern web applications, microservices architectures, and cloud-native SaaS are typically fine at any of the above latencies.

Failure modes worth designing for. Undersea cable cuts periodically affect India-to-Middle-East-to-Europe paths (the SEA-ME-WE cable system has multiple documented failures per year). Local fibre cuts on India's inland routes are more frequent than most parent CIOs expect. Bengaluru's specific micro-markets (Whitefield, Outer Ring Road, Electronic City) have had multi-hour connectivity events tied to construction. The correct architecture for resilience is dual-operator ILL with different last-mile paths, SD-WAN failover with sub-second convergence, and, for critical operations, an LTE/5G backup circuit that carries at least SASE-managed traffic during ILL outages.

Latency is a design variable, not a fact of physics you accept. For US-West parents, the answer is often India-local instances of the parent's key applications, secured through the parent's identity fabric but hosted in AWS Mumbai or Azure India, with data replicated back to parent regions on defined cadences. This is architectural work that has to be planned in the setup phase; retrofitting it after the parent CIO discovers the SAP client is unusable takes twice as long.

How Do You Build Hybrid Collaboration That Passes the 90-Day Test?

Parent-side executives form a lasting judgment about the India GCC in the first ninety days, and the single largest input to that judgment is whether meetings work. A parent CFO who joins three consecutive calls into the India office and cannot clearly hear the room decides, permanently, that "the India setup is not quite right yet" - and that judgment survives any technical fix delivered later. The collaboration architecture is not a comfort layer; it is the reputation layer.

Three design principles determine whether meetings work:

Platform parity with the parent. The GCC runs the same collaboration platform as the parent, Cisco Webex Suite, Microsoft Teams, or Zoom Workplace. Cross-platform interop (Webex-to-Teams, Zoom-to-Webex) is technically available and creates a 3-5% friction tax on every meeting that never goes away. The licensing savings from picking a different platform than the parent are consistently smaller than the cost of the friction.

Room hardware standardisation. GCC meeting rooms use the same room-hardware family as the parent's rooms, in the same room templates (huddle, medium, large, boardroom, executive). A parent employee joining a call to Bengaluru should see the same join button, hear the same audio quality, and be able to share the same way as they do in their home office. This is why we standardise on Cisco Room Kit series for Cisco-standard parents (Room Kit EQ for large, Room Kit Pro for boardroom, Room Bar for medium, Board Series for interactive), Microsoft Teams Rooms certified devices for M365-standard parents (Poly Studio X-series, Logitech Rally family, Yealink MeetingBar, Neat Bar, or Cisco with Teams Rooms mode), and Zoom Rooms certified devices for Zoom-standard parents.

Audio quality treated as an engineering deliverable, not a purchasing decision. Front-of-room audio failures, echo, dropouts, and unclear voices from the back of the room are the specific failure mode that damages the GCC's reputation with parent executives. This is a solvable engineering problem: proper acoustic design, correct microphone placement for the room shape, professional audio calibration, and Cisco Room Bar or Microsoft-certified equivalent room hardware with sufficient beamforming coverage. The budget is meaningful (₹8-25 lakh per large room, ₹4-8 lakh per medium room, ₹1.5-3 lakh per huddle room) and the return is measured in parent-executive trust.

Identity federation for single-touch join. Every meeting room joins parent-hosted meetings through the parent identity provider with a single tap. Every laptop signs into the collaboration platform through the same SSO the parent uses. The engineering here is unglamorous: SAML federation, conditional access policies, room-device certificates, and completely determinative of whether parent employees feel the India rooms are "part of the same estate" or "a separate world."

Operating rhythm is a design input, not a policy question. The collaboration architecture should reflect the sustainable meeting window for the parent geography. For CET parents, the India-CET overlap is typically 2 PM to 6 PM IST; design meeting rooms and studio spaces for that peak. For US East parents, the overlap is 8 PM to 9:30 PM IST for the India side or 6:30 AM to 8 AM ET for the parent side; the architecture should support asynchronous work (recorded room video with searchable transcripts through Cisco Vidcast, Microsoft Stream, or Zoom recordings) as first-class, not as an afterthought.

How Do You Meet DPDP, CERT-In, and Parent SOC Obligations from Day 1?

The India GCC entity acquires legal obligations on the day of incorporation, independent of when the technology infrastructure goes live. Three obligation streams matter for infrastructure: CERT-In Directions of 28 April 2022 (six-hour incident notification, 180-day log retention within India, mandatory NTP synchronisation to NIC or NPL time sources), DPDP Act 2023 with DPDP Rules notified 13 November 2025 (which apply the moment the entity processes personal data, and employee data qualifies from Day 1), and parent SOC integration (so the India entity does not become a monitoring blind spot in the global estate).

The three-obligation architecture.

- **Parent SOC feed.** Endpoint EDR, network flow, cloud telemetry, and identity events ingest into the parent SIEM through the parent's standard collectors, Microsoft Sentinel data connectors, Splunk Universal Forwarder, Chronicle SecOps ingestion, or the parent XDR of choice. This gets the India entity into the parent's global detection and response fabric on Day 1.

- **India SIEM view for CERT-In visibility.** A parallel or filtered view of the same telemetry, hosted in India, satisfies CERT-In's 180-day log retention requirement without requiring parent SIEM data to be repatriated. The specific pattern we use is a filtered tap of the parent SIEM feed into an India-hosted collector, the same events, retained locally, with an incident-response runbook that meets the six-hour notification obligation. This structure survives parent-SOC outages and keeps CERT-In evidence within Indian jurisdiction.

- **DPDP-aware data flows.** From Day 1, employee personal data (identity, payroll integration, endpoint attribution, access logs) is DPDP-in-scope. The architecture keeps employee identity data primary in India, with the parent identity fabric federating rather than repatriating. Where the GCC serves Indian customers (customer-support GCCs, India-market operations), customer personal data locality follows DPDP rules with documented cross-border transfer paths. For cross-border transfers of Indian personal data outbound to the parent, the applicable legal basis (contract, consent, or notified country) is enumerated and documented, not left as a legal-team-to-figure-out-later item.

- **Zero Trust access to parent applications.** Legacy full-tunnel VPN from India to parent networks is the pattern with the highest audit and DPDP exposure. Replace it with parent-standard ZTNA (Zscaler ZPA, Netskope Private Access, Cisco+ Secure Connect, or Cloudflare Access) with session-level authentication and posture assessment. This is a Day 1 architecture decision, not a Year 2 improvement.

- **NTP synchronisation.** Under the CERT-In Directions, mandatory synchronisation to Indian government time sources, NIC's NTP servers or the National Physical Laboratory (NPL) sources. This affects log timestamps across every layer and must be configured before the first log line matters for an incident. Trivial engineering, non-trivial audit consequence if missed.

- **Sector-specific overlays.** BFSI GCCs pick up RBI Master Directions applicable to the parent's Indian operations. Healthcare-adjacent GCCs handling Indian patient data pick up hospital-partner DPA requirements. Defence, aerospace, and telecom GCCs may pick up NCIIPC obligations if the parent's Indian operations are notified Critical Information Infrastructure. Confirm applicability with the parent's India regulatory counsel at setup.

What Does the Infrastructure Actually Cost?

The infrastructure component of a GCC setup, decoupled from real estate, entity setup, and people cost, lands in tighter bands than most other setup categories, because the reference architecture is well understood and the vendor pricing is transparent. The bands below are indicative Indian-market pricing in August 2026 for a 200-seat single-location GCC and should be treated as planning anchors, not quotations.

One-time infrastructure setup cost (200-seat GCC):

Category	Typical Range (INR)	Notes
WAN and cloud on-ramp (SD-WAN edge, dual ILL install, cloud interconnect setup)	₹40 lakh – ₹1.2 crore	Depends on parent SASE choice and cloud interconnect count
Campus LAN and Wi-Fi (switching, Wi-Fi 6E / Wi-Fi 7 access points, cabling)	₹90 lakh – ₹2.2 crore	30,000-40,000 sq ft with typical density
Meeting rooms (12-18 rooms, Cisco Room Kit / Teams Rooms / Zoom Rooms, acoustic design)	₹1.4 crore – ₹3.5 crore	Mix of huddle / medium / large / boardroom
Endpoint fleet (200 laptops, docks, monitors, peripherals)	₹4 crore – ₹6 crore	Depending on discipline mix and parent laptop standard
Identity, security, and management (Cisco Duo / ISE, EDR, MDM, SIEM tap, first-year licensing)	₹80 lakh – ₹2 crore	Assumes parent-standard tools; add-on if any India-specific licensing
Infrastructure programme, integration, and Go-Live support	₹60 lakh – ₹1.4 crore	Setup PMO, design, deployment, hypercare

Total one-time infrastructure setup for a 200-seat GCC: ₹4.1 crore – ₹9.9 crore, subject to parent standard choices, room count, and endpoint spec. This excludes real estate fit-out (rack rooms, IDF/MDF, structured cabling paths, typically ₹40-90 lakh included in the real-estate line, not here), entity setup, and people cost.

Ongoing infrastructure operating cost (annual, ex-people):

Category	Typical Range (INR per seat per year)
WAN (dual ILL, SASE licensing share, cloud interconnect)	₹28,000 – ₹55,000
Collaboration (platform licences, room maintenance, meeting analytics)	₹22,000 – ₹45,000
Endpoint (refresh amortisation, EDR, MDM, warranty, imaging)	₹35,000 – ₹65,000
Security (SIEM share, cloud security posture, patch management)	₹12,000 – ₹28,000
Managed services (network / collaboration / endpoint operations, if partner-run)	₹20,000 – ₹55,000

Total infrastructure operating cost per seat per year: **₹1.17 lakh – ₹2.48 lakh,** on top of real estate, facilities, corporate services, and people cost.

At 500-seat and 1,000-seat scale, per-seat infrastructure cost drops materially because WAN, security tooling, and meeting-room investments amortise across more users. Programmes designed for eventual 500-1,000 seat scale should specify the architecture for that target from Day 1 rather than sizing to the initial 200-seat requirement; retrofitting to scale costs more than building for scale.

What Infrastructure Mistakes Kill Trust with the Parent?

Four failure modes account for the majority of GCC infrastructure trust failures we have observed in the last four years. Each is entirely preventable with the right setup discipline.

Cheap meeting rooms. The single most common, and most damaging, infrastructure mistake. Rooms specified to save capex, delivered with consumer-grade cameras, single omnidirectional microphones covering a 20-seat conference table, and no acoustic treatment. Parent executives judge the GCC on these rooms. Within ninety days, "we can't quite hear you" becomes an unofficial verdict on the entire India operation. Recovery takes 12-18 months of rebuilding trust that a properly specified room would never have lost.

Single-underlay ILL that treats redundancy as a Phase 2 item. A single provider ILL "for now, with the second one to follow when we have budget headroom" is a scheduling error, not a cost saving. India's ILL market has enough operational variation that a single-underlay GCC will experience a multi-hour outage in its first quarter with 80%+ probability. That outage becomes a parent-side conversation about "India reliability" that is impossible to un-have.

Full-tunnel VPN as the parent-access mechanism. VPN is what the parent SOC has always done, so it is what the setup team does. Then the DPDP assessment or the parent's own Zero Trust programme catches it 12-18 months in, and the entire remote-access architecture has to be re-engineered, in production, with users on it. Deploy ZTNA from Day 1 through the parent's SASE fabric; do not deploy VPN and then retire it.

Making the India entity a SOC blind spot. The GCC ships endpoints, network, cloud, and identity telemetry to a shared drive or a local SIEM instance "until we integrate with the parent SIEM." The parent SOC never sees India events. When a Cisco Talos / Microsoft Threat Intelligence / CrowdStrike alert fires globally, the India entity is checked last, by a team that does not have the tooling. This is the failure mode that gets an India GCC written into a parent-side board-level cyber incident report. Ingest to the parent SIEM from the first endpoint enrolled, not from Month 6.

Frequently Asked Questions

How does Proactive engineer the network from an India GCC to parent HQ?

Dual-underlay ILL from independent Indian operators (typical pairings: Airtel + Tata Communications, Jio + Airtel), Cisco Catalyst SD-WAN or parent-standard SD-WAN overlay with application-aware policy routing, integration with parent SASE fabric (Zscaler, Netskope, Palo Alto Prisma Access, or Cisco+ Secure Connect with Umbrella) for parent-private application access via ZTNA, direct interconnect to AWS Mumbai and Hyderabad, Azure Central India (Pune) and South India (Chennai) and West India (Mumbai), and GCP Mumbai and Delhi. India-market internet uses local egress rather than SASE round-trips.

What is the round-trip latency from Bengaluru to parent HQ, and which applications will break?

Bengaluru or Hyderabad to Singapore or Hong Kong: 60-90 ms. To Dubai, Frankfurt, London, or Amsterdam: 130-180 ms. To US East: 190-230 ms. To US West: 230-260 ms. Modern web applications and cloud-native SaaS work fine at any of these ranges. Applications that break: chatty database protocols, legacy Windows client-server, specific CAD/EDA tools designed for LAN operation, older Citrix or RDP topologies. Solution is architectural rework or India-local instances of the parent stack.

Does Proactive support Cisco Webex, Microsoft Teams, and Zoom for GCC collaboration?

Yes. We design and operate hybrid meeting rooms on Cisco Room Kit series for Cisco Webex-standard parents, Microsoft Teams Rooms certified devices (Poly, Logitech, Yealink, Neat, or Cisco with Teams Rooms mode) for Microsoft 365 parents, and Zoom Rooms certified devices for Zoom Workplace parents. Platform parity between parent and GCC is a design principle; cross-platform interop is available but rarely optimal for daily operations.

How does Proactive meet CERT-In and DPDP obligations from Day 1?

Parent SIEM feed via standard collectors, plus a parallel India-hosted SIEM view for CERT-In's 180-day log retention within India. Incident response runbook meeting the six-hour notification obligation. NTP synchronisation to NIC or NPL time sources. DPDP-aware data flows keeping employee personal data primary in India with identity federation rather than repatriation. Zero Trust remote access replacing legacy VPN from Day 1. Sector-specific overlays for BFSI, healthcare, defence, or telecom GCCs where applicable.

What does the infrastructure cost for a 200-seat GCC in India?

One-time infrastructure setup: ₹4.1 crore – ₹9.9 crore across WAN, LAN and Wi-Fi, meeting rooms, endpoint fleet, identity and security, and programme management. Annual infrastructure operating cost per seat: ₹1.17 lakh – ₹2.48 lakh across WAN, collaboration, endpoint, security, and managed services. Excludes real estate, entity setup, and people cost. Per-seat cost drops materially at 500-seat and 1,000-seat scale.

Why This Guide, From Proactive

Every global CIO handed technology charge of an India GCC arrives with the same infrastructure question the entity-setup consultants, real-estate advisors, and tax firms do not answer: who actually builds and runs the network, collaboration, security, and identity on Day 1 and through the hire waves that follow?

Proactive Data Systems has been that partner for global parents standing up and operating India GCCs for over a decade, regardless of whether the entity was set up directly, through a BOT partner, or as a GCC-as-a-Service arrangement. We are a Cisco Preferred Partner across five portfolios — Networking, Security, Collaboration, Data Center, and Services, with the Cisco Advanced Customer Experience Specialised designation. Founded in Delhi NCR in 1991. Over 1,500 enterprise customers across India. More than 100 certified engineers. A dedicated GCC infrastructure practice with delivered engagements across Bengaluru, Hyderabad, Chennai, Pune, Delhi NCR, and Mumbai.

What we bring is the specific technology depth and Indian delivery experience that separates a GCC where meetings work, the network is up, applications reach parent systems predictably, and CERT-In and DPDP are covered from Day 1, from a GCC where any of those things becomes a Year 2 crisis.

When global CIOs compare us to alternatives, a global systems integrator's India arm, a big-four's technology practice, or a boutique India infrastructure specialist, three things typically decide the engagement.
First, we design network, collaboration, security, and identity as a single integrated architecture that operates from Day 1 and scales through 500 and 1,000 seats without re-architecture.
Second, we bring current, tested Indian-market vendor and telecom relationships, the specific Airtel account team who understands GCC needs, the Tata Communications capacity planners in the right city, and the AWS and Azure India teams who move interconnect requests on real timelines.
Third, our implementations produce evidence packs that satisfy both parent-side audit and CERT-In / DPDP from Day 1, not as a retrofit six months later.

If you have been handed technology charge of a new or growing India GCC, book a 30-minute conversation with a Proactive GCC infrastructure architect who has delivered the layer that actually keeps the centre running.

Talk to a GCC Infrastructure Architect

Disclaimer

This field guide is a working reference produced by the Proactive Data Systems GCC Practice for the use of global CIOs, CTOs, and Heads of Infrastructure responsible for the technology layer of an India Global Capability Centre. It covers network, collaboration, security, and identity infrastructure only. It does not cover entity setup, tax, real-estate, or HR - consult specialist advisors for those categories. Regulatory references (DPDP Act and Rules, CERT-In Directions, sector-specific frameworks) reflect the position at Version 2.0 of publication (August 2026) and may have changed since. Cost bands are Indian-market planning anchors, not quotations, and vary materially by location, specification, scope, and parent standard choices. Named third-party products and vendors are referenced for illustration only and do not constitute endorsement.

Proactive Data Systems is an enterprise IT infrastructure and services company. For more than three decades, the company has designed, deployed, and operated the technology foundations behind some of India's most demanding enterprise environments, from regulated industries to large distributed operations.

Founded in 1991, Proactive serves more than 1,500 customers, from fast-growing businesses to Fortune 500 enterprises, across banking and financial services, manufacturing, healthcare, public sector, IT and ITES, retail, education, and global capability centres. Our work spans enterprise networking, cybersecurity, cloud and AI-ready data centres, collaboration platforms, structured cabling, and managed services.

A Cisco Preferred Partner under the Cisco 360 Partner Program, Proactive is recognised across the Networking, Security, Collaboration, Cloud & AI, and Services portfolios, and is a Cisco Advanced Customer Experience Specialised Partner. The company is ISO 9001:2015 and ISO/IEC 27001 certified, and engineers solutions in partnership with Dell, Nutanix, NetApp, Palo Alto Networks, Fortinet, VMware, Veeam, and CommScope.

Headquartered in Delhi NCR, with offices in Mumbai, Bengaluru, Pune, Hyderabad, Indore, and Singapore.

To learn more about our solutions, write to us
at pro@proactive.co.in

www.proactive.co.in

PROACTIVE™
Enhancing Digital Experience