



JULY '26 INSIGHTS

Accelerated Computing Enterprise is the Indian arm of Cloud Ace Group.

Cloud Ace was established in Japan in 2014 and became the first Managed Service Provider (MSP) for Google Cloud in the country. Cloud Ace have won the Google partner of the year award in 2018 & 2021 as we continued to grow our business to other part of Asia and now we are expanding into Europe, North and South America as well as Africa.

We can help you in digital transformation by modernizing your infrastructure with best in-class cloud-native and cloud advisory services.

Inside This Issue

- Our Mission, Vision & Commitment
- Specialization
- Our Services
- Our Global Collaboration
- **Customer Advisory**
- **New Customer Success Stories**

Terms of Services

To learn more about our Service Terms, Policies, and Engagement Guidelines, please visit our official Terms of Services page:
<https://c-ace.co/cain-terms-of-service/>

10
Countries

600+
Experts

1000+
Happy Clients

OUR MISSION

Build our work on Honesty.

It is our mission with an unwavering pride that we are always aware of as we work to realize our vision; not just being honest, but “Honesty itself is our work and our service.”

OUR VISION

To contribute to building a world where all people can utilize advanced technology and realize the dreams they have envisioned.

We aspire to build a world where every person in the world can achieve their ambitions through the use of advanced technology. Our vision is to create such a world and help those who want to achieve it.

OUR COMMITMENT

As Google Cloud Partners, we are committed to providing our clients with cutting-edge technologies and exceptional customer service. Our team of experts is trained and certified to help you leverage the full potential of the Google Cloud Platform, from cloud storage and networking to machine learning and artificial intelligence.

SPECIALIZATION

This achievement reflects our continued commitment to delivering exceptional cloud solutions and deep technical expertise on the Google Cloud Platform (GCP). More importantly, it enables us to offer you enhanced support through Google Funding, specifically for any Engineer Support work related to GCP.

What this means for our Clients:

- Access to Google-backed funding to support your cloud engineering initiatives
- Priority support from certified experts across various GCP services
- Improved delivery capabilities and faster time-to-value for your projects
- Recognition that you're working with a trusted, Google-verified partner

We'd love to explore how we can leverage this specialization to add more value to your current or upcoming cloud initiatives. Please let me know a convenient time for a quick call or feel free to reply here — we're excited to help you get started.

Looking forward to continuing our collaboration with even more momentum!



SPECIALIZATION

Infrastructure

Google Cloud

OUR SERVICES



Managed & Consulting Services

Our Managed & Consulting Services Portfolio includes Cloud Infrastructure Services, Cloud Migration Assessment & Planning, Billing & Cost Optimisation, Monitoring, Security, Incident Management and on-going Support Activities.



System Migration, Design, Development & Automation

We provide Application Development, Modernisation Solutions, Cloud Migration Deployment & Optimisation, POCs, Infrastructure Orchestration & Continuous Improvement Activities.



Multi-Cloud, Hybrid Cloud, Backup & Recovery Solutions

If our Customers have Multi-cloud or Hybrid Cloud needs, as Google Cloud Partners, we can help them manage the most Complex Cloud Environments.



AI/ML, Gen AI, Data Engineering, Reporting & IoT Services:

We specialise in providing AI/ML and GenAI Solutions. We can also help our Customers with Data Warehousing, Data Analytics, Dashboarding & Reporting Solutions on top of Google Cloud's Data Services.



Training & Adaptation

Our Certified Professional Google Certified Trainers can help you in Training to ensure that your Team & your Customers are Knowledgeable in GCP & GWS Best Practices, which can inspire Client Confidence.



Google Workspace

We provide Google Workspace Deployment & Migration Business Solutions for setting up Gmail, Google Drive, Google Calendar and other Productivity tools.

OUR GLOBAL COLLABORATION

Expanding Our Global Collaboration to Strengthen Google Cloud Project Delivery in India

At Cloud Ace, we take pride in being one of the leading Google Cloud Partners globally, with a strong footprint across multiple markets. As a Japanese cloud technology company, our commitment to delivering high-quality cloud solutions has always been at the heart of everything we do.

In India, the demand for Google Cloud SI&C (System Integration & Consulting) projects continues to grow rapidly. To ensure we meet and exceed client expectations while maintaining the highest standards of delivery, we are now actively collaborating with our global divisions—including teams from Japan, Vietnam, Hong Kong, and Indonesia.

This strategic collaboration allows us to leverage engineering talent and technical expertise across borders, enhancing our delivery capabilities and ensuring timely execution of projects in India. By aligning with our overseas teams, we aim to bring the best of global knowledge and experience to our local engagements.

This is a significant step forward in our mission to provide reliable, scalable, and future-ready Google Cloud solutions to enterprises in India.

Together, across borders, we continue to build smarter with the cloud.

Customer Advisory

Securing Your Google Cloud Environment and Monitoring Usage

This advisory is being shared to help customers reduce the risk of unauthorized access, misuse of cloud resources, and unexpected billing impact in Google Cloud.

Cloud Ace India acts as a billing reseller and invoice issuer for Google Cloud consumption. Unless separately agreed in a managed services, security monitoring, or workload operations contract, Cloud Ace India does not administer, continuously monitor, or operate customer workloads, identities, APIs, projects, or data environments on a 24×7 basis.

Customers remain responsible for the security configuration, identity controls, API usage, quota governance, workload monitoring, logging, and incident response inside their own Google Cloud environment. This advisory is intended as general best-practice guidance and is not an exhaustive security standard or guarantee against misuse or loss.

Important note on billing and usage alerts

Budget alerts and anomaly signals are useful detective controls, but they should not be treated as real-time preventive protection. Billing-based signals can lag behind actual usage, which means unauthorized or abusive consumption may already have occurred before alerts are visible.

Official Google documentation:

- Create, edit, or delete budgets and budget alerts
- View and manage cost anomalies
- Set up programmatic notifications

Minimum actions we recommend customers review immediately

1. Enforce multi-factor authentication for all privileged and active users

Passwords alone are not sufficient protection for administrative access.

Customers should ensure multi-factor authentication is enforced for privileged users and, where practical, broadly across active users in the organization. For highly sensitive administrator accounts, phishing-resistant methods such as hardware security keys should also be considered.

Official Google documentation:

- 2-step verification requirement for Google Cloud
- Deploy 2-Step Verification
- Manage a user's security settings

2. Review account recovery settings and Google Essential Contacts

Recovery phone numbers, recovery email addresses, and Google Essential Contacts should be current and actively monitored. During a security or billing incident, outdated recovery settings or stale contact points can delay response and escalation.

Official Google documentation:

- Set up recovery options
- Essential Contacts overview
- Manage Essential Contacts

3. Secure API keys, secrets, and service account credentials

Customers should avoid storing credentials in source code, documents, or unsecured locations. Sensitive values should be stored in a secure secrets-management solution. API keys should never remain unrestricted; they should be limited to the required APIs and constrained using appropriate environment restrictions where supported. User-managed service account keys should be minimized, rotated, and disabled where not required.

Official Google documentation:

- Manage API keys
- Secret Manager documentation
- Authentication and authorization guidelines

4. Configure budgets, anomaly detection, and monitored notification paths

Customers should configure billing budgets and cost anomaly notifications and route them to actively monitored distribution lists or responsible operational owners. These controls improve awareness of unusual consumption, but they do not replace preventive access controls, quota management, or customer-side monitoring.

Official Google documentation:

- Create, edit, or delete budgets and budget alerts
- View and manage cost anomalies
- Set up programmatic notifications

5. Review quotas and access for high-cost or high-risk services

Customers should review whether high-cost resources and high-risk services are enabled only where needed, and whether quota levels are appropriately limited. This is especially important for workloads that can scale rapidly or generate high consumption in a short period of time.

Official Google documentation:

- View and manage quotas
- Quota permissions
- Access control with IAM for Service Usage

6. Enable and retain audit logging

Customers should ensure relevant audit logs are enabled and retained in a durable location to support investigation and incident response. Logging is critical for understanding who performed an action, what changed, and when activity occurred.

Official Google documentation:

- Cloud Audit Logs overview
- Configure log buckets
- Route log entries

7. Use native Google Cloud security controls where applicable

Depending on the environment and workload profile, customers should evaluate native security capabilities such as Security Command Center, Identity-Aware Proxy, Cloud Armor, and other Google Cloud security services that help reduce attack surface and improve visibility.

Official Google documentation:

- Google Cloud security best practices catalog
- Security Command Center best practices
- Organization Policy Service roles and permissions

8. Maintain an internal incident-response owner and process

Customers should define who receives security and billing alerts, who can take immediate containment actions, and who is responsible for reviewing logs, rotating credentials, and coordinating escalation during an incident. Rapid response inside the customer environment remains essential.

Official Google documentation:

- Respond to alerts and cases
- Security Command Center documentation
- Compliance Manager cloud controls

Recommended customer operating model

Customers should ensure that:

- named owners exist for IAM and privileged access management
- billing alerts are sent to monitored operational contacts
- quota increases are reviewed and approved through an internal process
- unused projects, resources, keys, and accounts are reviewed periodically
- high-risk services are enabled only when justified by business need
- incident contacts and escalation paths are documented and tested

Cloud Ace India scope

Under the standard billing reseller model:

- Cloud Ace India can provide billing visibility and invoice-related communication based on the billing data available to us
- Cloud Ace India may notify customers when billing-side monitoring identifies unusual patterns after relevant usage data becomes available
- such notifications are advisory in nature and depend on billing telemetry timing and the visibility available at the billing layer
- Cloud Ace India cannot guarantee real-time detection, prevention, or containment of unauthorized activity occurring within customer-managed workloads or projects
- investigation, remediation, IAM changes, API restrictions, quota changes, workload shutdown, and forensic review remain the customer's responsibility unless separately contracted as a managed service

Closing note

We recommend that each customer review the above items with their internal cloud, security, and operations teams and implement controls appropriate to their environment, workload profile, and risk posture.

This advisory is intended to support customer awareness and best-practice adoption. It does not replace the customer's own security governance, monitoring, or incident-response obligations.



NEW CUSTOMER SUCCESS STORIES

Software Development Company | Chandigarh

We partnered with a Chandigarh-based software development company to support their high-performance GPU requirements on Google Cloud. Our team helped them optimize cloud infrastructure while reducing their overall monthly cloud expenditure.



Law Firm | Pune

A leading Pune-based law firm selected Cloud Ace India to implement Gemini Enterprise for secure document management and client data handling. Given the highly confidential nature of their business, we provided expert guidance on solution architecture, security, and Gemini Enterprise adoption.

Export Company | Karur, Tamil Nadu

We onboarded a leading export company to accelerate AI adoption using Gemini Enterprise. Our solution focused on automating workflows, enhancing product visualization, improving collaboration across design, finance, and marketing teams, and integrating seamlessly with their existing Microsoft 365 environment.

Recruitment Services Company | Bengaluru

We helped a Bengaluru-based recruitment services company successfully migrate from Google AI Studio to Vertex AI. In addition to ensuring a smooth migration, we optimized their Google Cloud environment to improve performance while reducing monthly cloud costs.

AI & Cloud Training Provider | Pune

A Pune-based AI and Cloud training provider partnered with Cloud Ace India to resolve Google Cloud quota limitations on their direct billing account. As a Google Cloud Premier Partner, we successfully addressed the quota challenges while optimizing their cloud spending for improved operational efficiency.



Accelerated Computing Enterprise Pvt. Ltd.

Delhi NCR

www.c-ace.co | in@cloud-ace.com

Cloud Ace Global | Japan, China, Hong Kong,
Taiwan, Thailand, Vietnam, Singapore, Indonesia,
India, and Brazil.

View Terms of Services: <https://c-ace.co/cain-terms-of-service/>